INTELLIGENCE ARTIFICIELLE D'ENTREPRISE

Développer une IA de confiance dans le cloud souverain

Shannon Bell
David Fraser
Tom Jenkins

INTELLIGENCE ARTIFICIELLE D'ENTREPRISE

Développer une IA de confiance dans le cloud souverain

Par Shannon Bell, David Fraser et Tom Jenkins

Première publication, novembre 2025

Publié par

Open Text Corporation

275 Frank Tompa Drive

Waterloo, Ontario, Kanada

N2L 0A1

(519) 888-7111

info@opentext.com | www.opentext.com

Préface

James Arroyo OBE
Ancien directeur des données au ministère britannique des Affaires étrangères et du Commonwealth et directeur de la Fondation Ditchley

Nous sommes à un tournant de l'histoire – à une époque où les systèmes technologiques du monde convergent, soulevant des questions de pouvoir, de confiance, de souveraineté et de gouvernance. L'intelligence artificielle est en train de redéfinir la manière dont les décisions sont prises, dont les entreprises fonctionnent et dont les sociétés opèrent. Pourtant, les progrès de l'IA ne peuvent pas être mesurés uniquement en fonction des capacités techniques. Nous devons associer ses progrès à des principes clairs, à la discipline éthique et à une nouvelle compréhension de ce que signifie la souveraineté à l'ère numérique.

Ce livre, *L'intelligence artificielle d'entreprise : Développer une IA de confiance dans le cloud souverain*, aborde à la fois les défis et les opportunités que représente l'IA. Il admet que la prochaine décennie sera définie non seulement par ceux qui élaboreront les plus grands modèles, mais aussi par ceux qui gouverneront et utiliseront les données le plus efficacement possible. Les données sont à la fois le moteur et le fondement des systèmes d'intelligence modernes. Tout comme l'énergie ou les devises, elles nécessitent des réglementations, une gestion responsable et, surtout, de la confiance. L'avenir de l'IA dépend de la manière dont nous gérons la confidentialité, l'origine et la souveraineté de ces données. Cela deviendra essentiel à mesure que les particuliers, les institutions et les entreprises s'apprêtent à ajouter leurs propres données personnelles, exclusives et souveraines, aux systèmes d'IA.

Lorsque j'étais directeur des données au ministère des Affaires étrangères et du Commonwealth du Royaume-Uni, notre mission ne consistait pas simplement à numériser l'institution et à définir les politiques qui rendraient la transformation numérique viable pour les décennies à venir. Nous avons dû nous poser des questions difficiles : *À qui appartiennent les données sur lesquelles nous nous appuyons ? Où résident-elles ? Comment sont-elles partagées, stockées et sécurisées ? Combien de temps doivent-elles être conservées ?* Ces mêmes questions se posent désormais à toutes les entreprises, à tous les gouvernements et à tous les citoyens, alors que les systèmes d'IA deviennent de plus en plus autonomes et omniprésents. Les pouvoirs d'inférence de l'IA signifient que chaque atome de données peut potentiellement apporter des informations sous forme de combinaison agrégée, et c'est ce qui change la donne.

Au fil des discussions avec les dirigeants du secteur technologique, des pouvoirs publics et de la société civile, il apparaît clairement que la politique en matière de souveraineté des données n'est pas un débat technique, mais une question de sécurité nationale et économique. Dans un monde où la majorité des données sont protégées par des pare-feu d'entreprise et gouvernementaux, la souveraineté s'étend au-delà de la simple conformité. C'est une question de contrôle, de responsabilité et de capacité à agir en toute confiance dans un monde où les décisions sont prises par des algorithmes.

* Le point de vue de James Arroyo ne reflète pas nécessairement celui de la Ditchley Foundation.

Ce livre présente des arguments convaincants en faveur de cette philosophie. Il affirme que des données fiables et une IA responsable sont les deux faces d'une même médaille, et que pour développer une IA équitable, explicable et sûre, nous devons nous assurer que les données dont elle s'alimente sont bien gérées, contextualisées et souveraines. Sans protection de la vie privée et sans gestion des données, l'IA risque de fragiliser les institutions qu'elle cherche à renforcer. Sans innovation, la gouvernance risque de devenir un obstacle au progrès. La tâche qui nous attend est d'aligner confiance et innovation afin que l'un renforce l'autre.

Au fil de votre lecture, vous verrez comment le paysage informatique d'entreprise est reconstruit de fond en comble. Les infrastructures à très grande échelle, les clouds souverains et les systèmes basés sur l'IA constituent l'infrastructure essentielle du maillage industriel de l'économie numérique. Mais le véritable avantage reviendra à ceux qui traitent les données non pas comme une marchandise neutre, mais comme un principe constitutionnel – les données doivent être protégées, respectées et déployées de manière responsable.

Je soutiens chaleureusement l'appel à l'action du livre : agir vite, mais gouverner plus vite ; innover avec audace, mais avec détermination ; faire en sorte que chaque avancée numérique renforce la confiance du public au lieu de l'éroder. C'est l'essence même du leadership dans cette nouvelle ère de l'IA.

Dans les années à venir, les pays et les entreprises qui vont gagner, en intégrant l'IA dans la société et en encourageant son adoption généralisée et approfondie, seront ceux qui comprendront une vérité simple mais profonde : **une IA sans confiance, sans souveraineté et sans une bonne gouvernance des données, c'est un pouvoir sans responsabilité, et peut-être sans légitimité**. Mais lorsque l'innovation et la gouvernance évoluent au même rythme, lorsque la confidentialité, la responsabilité et l'éthique sont intégrées à la conception, nous pouvons créer non seulement des systèmes intelligents, mais aussi des sociétés intelligentes.

L'ère de l'informatique cognitive est arrivée, une époque où la confiance est le fondement et où l'innovation est le moteur. Son succès ne dépendra pas uniquement des machines, mais de notre capacité commune à définir les principes qui les régissent. *L'intelligence artificielle d'entreprise : Développer une IA de confiance dans le cloud souverain* offre une feuille de route pour ce voyage et une invitation à façonner l'avenir de manière responsable, ensemble.

À propos des auteurs

Shannon Bell

Shannon Bell est vice-présidente exécutive, directrice du numérique et directrice des systèmes informatiques d'OpenText. Elle est responsable des systèmes informatiques et numériques, des plateformes de données, des réseaux et des communications, des opérations cloud commerciales et d'entreprise, ainsi que de sa sécurité et de sa conformité. C'est une responsable informatique accomplie qui possède plus de 25 ans d'expérience internationale dans les domaines de la transformation technologique et des intégrations à grande échelle. Avant de rejoindre OpenText, elle a occupé un poste de direction chez Rogers Communications, où elle a dirigé l'intégration technologique lors de l'acquisition de Shaw. Au cours de sa carrière, elle a notamment occupé des postes chez Amdocs, NewStep Networks, MetaSolv Software, Axiom Systems et Newbridge Networks. Shannon est titulaire d'un MBA de l'université de Surrey et d'un diplôme de premier cycle de l'université Carleton.

David Fraser

Major-General (Ret.) Le major général (ret.) David Fraser est directeur d'OpenText depuis septembre 2018. Il est l'un des généraux les plus décorés de l'histoire des Forces armées canadiennes, et a notamment reçu l'Ordre du mérite militaire. En 2006, il était commandant de la brigade multinationale pour le commandement régional dans le sud de l'Afghanistan où il a dirigé l'opération Medusa, le plus important engagement en combat des Forces armées canadiennes depuis plus de cinquante ans. Le général Fraser a également été commandant du Collège d'état-major des Forces canadiennes. Après avoir pris sa retraite de l'armée, il a occupé un poste de cadre dans trois entreprises différentes, dont Blue Goose Pure Foods, et a acquis son expérience de leadership tant sur le champ de bataille que dans les salles de réunion. David a co-écrit *The Anticipant Organization*, un guide de survie destiné aux grandes entreprises dans un monde en constante évolution, avec Tom Jenkins et Mark J. Barrenechea.

Tom Jenkins

Tom Jenkins, l'un des plus grands experts canadiens en matière d'innovation et de technologies numériques, est le président d'OpenText Corporation, la plus grande société de logiciels et de cloud de l'histoire du Canada – l'une des sociétés Internet les plus prospères au monde. Tom a siégé ou continue de siéger aux conseils d'administration d'OpenText Corporation, de Manulife Financial, de Thomson Reuters, de TransAlta Corporation, de BMC Corporation et de Slater Steel. Il a également été président du Conseil national de recherches du Canada. Il a été nommé officier dans les Forces armées canadiennes et colonel honoraire d'un régiment d'infanterie et d'un escadron de chasseurs dans les Forces armées canadiennes. Il a été le 10e chancelier de l'université de Waterloo et il a été intronisé au Temple de la renommée des affaires canadiennes en tant que compagnon. Tom est récipiendaire de l'Ordre du mérite de la République fédérale d'Allemagne (Croix de chevalier) et il est officier de l'Ordre du Canada. Tom est l'auteur de nombreux livres économiques sur l'innovation numérique et a co-écrit *Ingenious : How Canadian Innovators Made the World Smarter, Smaller, Kinder, Safer, Healthier, Wealthier, and Happier, avec David Johnston*, l'ancien gouverneur général du Canada.

Remerciements

Les auteurs tiennent à remercier les personnes suivantes pour leur temps, leur énergie et leur perspicacité :

Michael Acedo, DeeDee Andrews, James Arroyo, Savinay Berry, Lev Dranikov, Paul Duggan, Joe Dwyer, Adam Hennessy, Bita Houshmand Rabiee, Michelle Kelly, Anupam Khazanchi, Edward Kiledjian, Mark L'Heureux, Stephen Ludlow, James McGourlay, Sandy Ono, Sunnie Rothenburger, Scott Schultz, ainsi qu'Elizabeth Chestney-Hanson, éditrice, Stephen Ksiadz et Kevin Sy, pour la mise en page et le design et Colombo Translation Ltd., pour la traduction.

Sommaire

Présentation

Bienvenue dans l'ère de l'informatique cognitive

Nous vivons un autre tournant technologique majeur : le début de l'ère de l'informatique cognitive, sous l'impulsion de l'essor de l'intelligence artificielle d'entreprise (IAE). Ce qui a commencé comme une révolution numérique s'est transformé en quelque chose de bien plus dynamique : un monde où les données ne servent pas seulement à éclairer les décisions, mais influencent également la technologie pour qu'elle interprète, apprenne et agisse.

Au cours des dernières décennies, les bases du secteur informatique ont changé. La pandémie de COVID-19 a contraint des économies entières à se numériser presque du jour au lendemain. L'adoption du cloud, le télétravail et l'automatisation ont progressé de manière significative en quelques mois seulement, plutôt qu'en plusieurs années. Le résultat ? Un paysage commercial complètement repensé dans lequel l'infrastructure numérique n'est pas simplement une couche opérationnelle, mais le cœur de l'entreprise.

Il n'y a pas si longtemps, l'informatique d'entreprise impliquait des serveurs improvisés fonctionnant dans des placards surchauffés, où une mauvaise ligne de code pouvait faire planter un système entier. Aujourd'hui, ces configurations fragiles ont été remplacées par une infrastructure à grande échelle, mondiale, résiliente et à l'évolutivité infinie. En plus de cette infrastructure essentielle, une nouvelle intelligence a vu le jour. L'intelligence artificielle (IA) agentique peut raisonner, s'adapter et réagir en temps réel. Le travail qui nécessitait auparavant des équipes de développeurs, de spécialistes du marketing ou d'analystes peut désormais être coordonné instantanément pour des millions d'utilisateurs.

Les applications d'entreprise classiques sont en pleine transformation

- Les hyperscalers s'attaquent au secteur B2B avec des services à faible coût dans le cloud.
- Le « fossé » du château est constitué des interfaces graphiques et des workflows (gestion de la configuration) de l'application.
- Le « mur » du château correspond aux données historiques contenues dans les archives qui sont nécessaires à la formation d'AI.
- L'avènement de l'intelligence artificielle agentique risque de compromettre ces deux défenses.

Les applications d'entreprise classiques sont en train de se transformer

Le nouveau point d'inflexion est la convergence de l'informatique à grande échelle et de l'IA agentique. Les hyperscalers et les clouds souverains sont devenus le réseau industriel de l'économie numérique, le pouvoir qui fait fonctionner tout le reste. Ajoutez à cela l'intelligence artificielle, et vous obtenez un système nerveux pour les entreprises modernes, qui ne se contente pas de stocker et de traiter des données, mais qui les anticipe et agit en conséquence. Pour les entreprises, il ne s'agit pas simplement d'une nouvelle vague d'innovation ; il s'agit d'une redéfinition complète de la manière dont le travail, la valeur et le renseignement circulent.

Les applications d'entreprise classiques évoluent rapidement pour suivre le rythme. Des hyperscalers tels qu'Amazon Web Services, Google Cloud et Microsoft Azure s'implantent dans le bastion traditionnel du B2B, proposant des services cloud performants et peu coûteux qui redéfinissent les règles du jeu. Pendant des années, ce qui a assuré la sécurité de ces systèmes était les éléments qui les rendaient difficiles à reproduire : leurs flux de traitement complexes, leurs interfaces personnalisées et leurs volumes considérables de données historiques conservées dans des archives sécurisées. Cependant, c'est précisément là que la nouvelle pression s'intensifie.

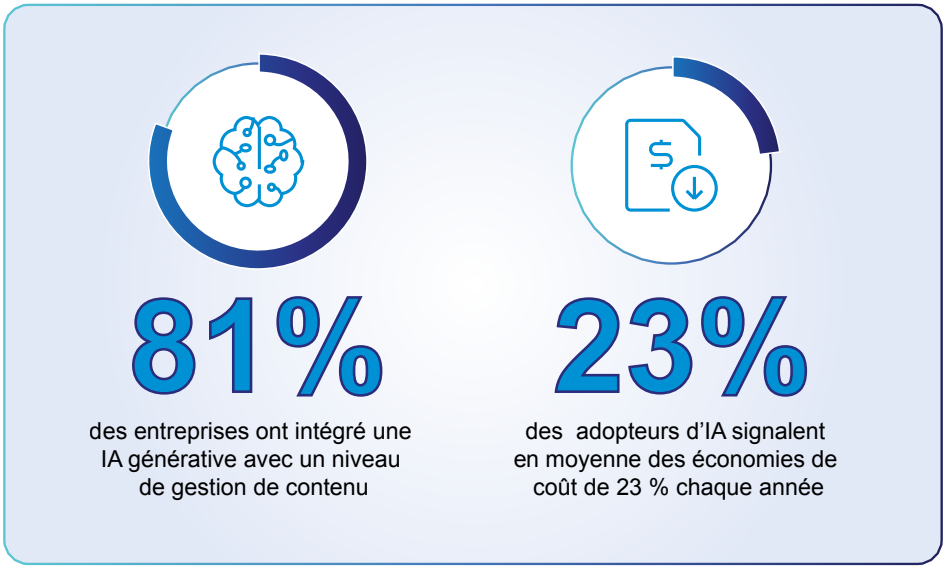
Ces anciennes défenses ne sont plus aussi efficaces qu'auparavant. Les interfaces utilisateur et les outils de configuration qui semblaient autrefois uniques peuvent désormais être reproduits en quelques minutes. Et les données conservées dans les archives, qui regroupent des années de transactions, d'interactions et d'enregistrements, sont devenues le carburant dont chaque modèle d'IA souhaite s'inspirer. L'IA agentique ne se contente pas de rivaliser avec les systèmes d'entreprise : elle apprend d'eux, les imite et, dans de nombreux cas, les surpasse.

L'avantage réel aujourd'hui ne réside pas dans la construction de murs plus hauts, mais dans la construction de fondations plus intelligentes. Ce qui rend une entreprise résiliente aujourd'hui, ce n'est pas la taille de son ensemble de technologies, mais la capacité avec laquelle elle gère, protège et exploite les données qu'elle contient. C'est là que commencent la véritable intelligence et la véritable différenciation.

Les leaders qui promeuvent l'informatique cognitive doivent trouver un équilibre entre confiance et innovation, en admettant que des données sécurisées et bien gérées soient le fondement de la confiance, tandis que l'IA est le moteur du progrès et de l'innovation. Des données fiables garantissent la confiance, la fiabilité et la conformité alors que l'IA permet de découvrir de nouvelles solutions et de gagner en efficacité. Sans une solide gouvernance des données, les progrès rapides de l'IA peuvent compromettre la confidentialité et la sécurité ; mais sans innovation, les progrès sont au point mort.

À l'heure actuelle, confiance et innovation doivent aller de pair. En alignant des pratiques rigoureuses en matière de données sur des initiatives audacieuses en IA, les entreprises peuvent exploiter de manière responsable les technologies transformatrices, en veillant à ce que chaque avancée repose sur la confiance du public et le respect de normes éthiques.

En termes simples, seules des données fiables peuvent alimenter une IA véritablement fiable et efficace.



Les primo-utilisateurs bénéficient déjà de l'adoption de l'IA intégrée [1]

La prochaine décennie sera celle des entreprises qui comprendront ce changement. Celles qui considèrent les données non pas comme un sous-produit de l'activité, mais comme son système d'exploitation. Celles qui comprennent que les données ne peuvent être efficaces que si elles sont fiables, contrôlées et sécurisées. L'IA transformera tous les secteurs, mais uniquement si elle repose sur des bases suffisamment solides pour y parvenir.

Réfléchissez à ceci : en mai 2025, Salesforce a annoncé son intention d'acquérir Informatica pour environ 8 milliards de dollars américains, un événement marquant qui nous indique précisément où se déplacent les lignes de front dans le domaine des logiciels d'entreprise. *Pourquoi cet accord était-il judicieux ?* Bien que Salesforce s'appuyait sur des systèmes externes pour ses données critiques, ses capacités d'intégration des données étaient limitées. Et l'entreprise voulait combler le déficit d'intégration des données afin que l'IA puisse fonctionner sur la base d'informations contextuelles et gouvernées.

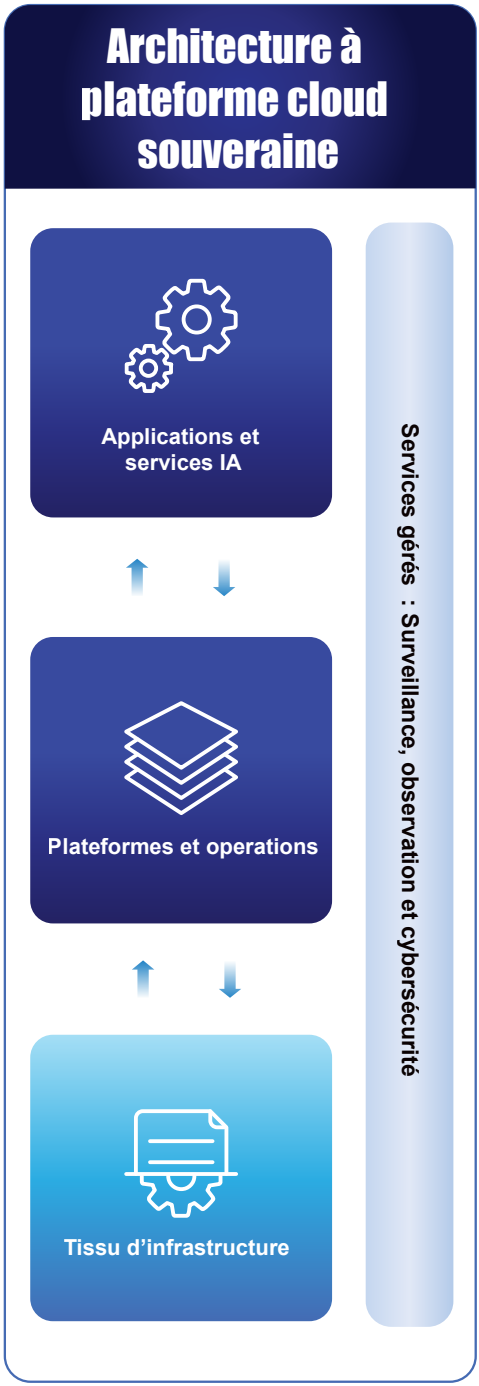
Salesforce a compris que l'avenir de l'IA dépendait de l'accès à des données sécurisées, structurées et non structurées, c'est-à-dire le type de données qui se trouvent au cœur des entreprises, et non sur le Web public. Cela est particulièrement vrai pour la formation aux systèmes *d'IA agentiques*, qui devraient devenir la pierre angulaire de la productivité des entreprises mondiales au cours de la prochaine décennie. Mais voici le défi : la plupart des informations les plus précieuses au monde ne se trouvent pas dans des sources de données publiques. Elles se trouvent au cœur des entreprises, des gouvernements et des institutions, où elles sont régies, protégées et souvent réglementées par la loi.

Les chatbots publics tels que ChatGPT, Claude et Perplexity ont déjà été formés sur presque toutes les informations librement accessibles : publications Reddit, pages Wikipédia et autres référentiels ouverts. Lorsqu'ils atteignent les limites de ce contenu et tentent de tirer des leçons d'informations plus spécialisées, ils entrent en conflit avec les limites du droit d'auteur, de la confidentialité et de la propriété des données. Il s'agit de *données propriétaires*, c'est-à-dire d'informations sur lesquelles les entreprises ont un droit de propriété, et qui sont de plus en plus soumises à des réglementations strictes en matière de confidentialité et de sécurité, qu'il s'agisse de cadres municipaux et fédéraux ou de normes mondiales établies par l'ONU et l'OTAN.

En réalité, plus de 90 % des données du monde se trouvent derrière les pare-feu des entreprises et des gouvernements. [2] Elles ne sont pas seulement difficiles à atteindre, elles sont également conçues dès le départ pour être protégées. Leur accès nécessite des autorisations, le respect de normes et de la gouvernance. C'est là qu'intervient la gestion des informations d'entreprise : les systèmes de gestion des documents et des dossiers, les flux de traitement et moteurs de règles qui contrôlent qui peut voir quoi, quand et pourquoi. Pour que l'IA agentique d'entreprise évolue de manière responsable, elle devra apprendre non seulement à partir des informations, mais également dans le cadre des garde-fous de confiance que fournissent ces systèmes.

Lorsqu'une entreprise entraîne ou peaufine son modèle de langage, large ou petit, à partir de données qu'elle n'a pas le droit d'utiliser, elle enseigne à la machine le travail de quelqu'un d'autre, et cela ne finit jamais bien. S'il s'avère que ces données sont exclusives, les retombées ne seront pas une petite réparation – il s'agira d'une réinitialisation complète. L'entreprise qui en est propriétaire peut exiger que l'IA soit « désentraînée », ce qui, dans le monde d'aujourd'hui, signifie repartir de zéro. Vous ne pouvez pas simplement retirer une mauvaise source de données, vous devez remonter là où l'erreur a commencé. Cela peut coûter des millions de dollars et des mois de temps perdu. Dans certains cas, un programme d'IA prometteur peut être immédiatement éliminé. Bref, lorsqu'il s'agit de gérer les données pour créer des modèles d'IA efficaces, les entreprises doivent y réfléchir à 2 fois. C'est pourquoi il est devenu essentiel de bien comprendre la souveraineté des données.

Chaque entreprise possède quelque chose de trop précieux pour le perdre : ses connaissances et ses données institutionnelles, les « clés du château ». C'est ce qui fait de votre entreprise la vôtre. Si vous les confiez au mauvais système ou au mauvais partenaire, vous risquez de voir vos propres informations vous revenir, reconditionnées et revendues. Les gouvernements sont également conscients de ce risque, c'est pourquoi ils s'empressent d'installer des garde-fous. De nouvelles lois relatives à l'intelligence artificielle et à la protection des données sont en cours d'élaboration, et elles donneront l'impression que le Règlement général sur la protection des données (RGPD) n'était qu'un prélude. Elles redéfiniront la façon dont les entreprises stockent, partagent et s'entraînent sur les données, en particulier lorsque des informations personnelles ou sensibles sont en jeu.



Les entreprises ont besoin de données souveraines

Pour se préparer à l'IA, les entreprises doivent comprendre les trois types d'ensembles de données qui alimentent les systèmes intelligents et les gérer de manière responsable :

1. Le contenu généré par l'homme que nous créons quotidiennement : documents, courriels, présentations, images, vidéos et conversations, ou ce que nous appelons la trace vivante de la pensée d'une entreprise.

2. Le contenu généré par des machines : fichiers de journalisation, alertes et télémétrie provenant des systèmes informatiques, des réseaux et des outils de sécurité – le bruit de fond continu du fonctionnement d'une entreprise.

3. Les données qui circulent entre les entreprises : transactions, échanges de fournisseurs et intégrations B2B. C'est le tissu conjonctif qui permet à l'économie de fonctionner.

L'IA d'entreprise agentique nécessite ces trois ensembles de données pour fonctionner dans un contexte commercial réel. Il s'agit de passer du *contenu contextuel à l'IA contextuelle*, où l'intelligence ne se contente pas de traiter des données, mais comprend également les relations, les intentions et la valeur afin d'agir efficacement et d'apprendre. Et tout comme les informations dont elle tire des leçons, l'IA elle-même doit être sécurisée, gouvernée et être en conformité. Il ne s'agit pas seulement de normes techniques, mais des fondements de la confiance qui déterminent si l'IA peut être utilisée en toute sécurité au sein de l'entreprise.

La vraie question n'est pas de *savoir si* vous allez partager vos données, *mais comment* vous allez en garder le contrôle.

La véritable souveraineté, c'est savoir où se trouvent vos données, qui y accède et comment elles sont utilisées – pas une seule fois, mais en permanence. Vous avez besoin de moyens sécurisés pour intégrer l'IA générative (GenAI), là où se trouvent déjà vos informations, au sein de vos systèmes sécurisés et gouvernés. Permettez à vos utilisateurs de discuter avec leur contenu : trouvez-le, résumez-le et développez-le sans jamais enfreindre les règles de gouvernance. Et transformez l'analytique en un sujet sur lequel vous pouvez simplement poser des questions dans un langage simple. Et introduisez en toute sécurité d'autres produits dotés des mêmes informations dans le domaine de la cybersécurité, de la gestion des applications, etc.

Avec des données sécurisées, gouvernées et souveraines, vous n'avez pas à céder les joyaux de votre couronne pour innover. Vous pouvez utiliser l'IA en toute confiance. Car à l'ère de l'intelligence responsable, les intelligence les plus performantes ne sont pas celles qui fournissent le plus de données à l'IA. Ce sont celles qui savent à quelles données se fier.

La voie à suivre : un appel au leadership

Comme nous en avons discuté, la prochaine ère d'innovation ne sera pas menée par ceux qui agiront le plus vite, mais par ceux qui agiront de manière la plus responsable. C'est l'intersection de la confiance et de l'innovation.

Chaque décision de l'exécutif, chaque ligne de code, chaque modèle d'IA comporte désormais une dimension morale, car l'information détient un pouvoir, et la manière dont ce pouvoir sera utilisé définira la décennie à venir.

C'est maintenant que les dirigeants d'entreprises, les pouvoirs publics et les industries devront considérer leurs données et informations non seulement comme une ressource, mais aussi comme une responsabilité. De renforcer les bases des données, intégrer la gouvernance à la conception et faire de la sécurité la solution par défaut, et non l'exception. L'avenir de l'IA dépend non seulement du degré d'automatisation, mais aussi de la confiance que nous pouvons accorder aux systèmes et aux données sur lesquels nous la construisons.

Dans tous les secteurs, nous sommes confrontés au même défi : la nécessité de transformer rapidement sans pour autant sacrifier le contrôle. Les entreprises qui réussiront seront celles qui allient le courage d'innover à la discipline nécessaire pour gouverner. Ce seront celles qui protègent la confidentialité avec autant de détermination qu'elles recherchent la perspicacité, qui font de la transparence un avantage concurrentiel et qui développent une IA d'entreprise capable non seulement de raisonner, mais aussi de gagner la confiance.

C'est là que la préparation rencontre la responsabilité. Où l'ambition numérique devient une intelligence responsable. Et où les technologies les plus transformatrices sont également guidées par des principes.

Tout comme les données fiables constituent le fondement et l'innovation en matière d'IA et éclairent la voie à suivre, les chapitres suivants présenteront les cadres de traitement données, les modèles de gouvernance de l'IA et les considérations clés pour les architectures de données souveraines et non souveraines. À la fin de chaque chapitre, vous trouverez une liste « Fast Five Download », des outils qui résument les points essentiels pour une consultation rapide, vous permettant ainsi d'être prêt à créer, gérer et innover en toute confiance.

La décennie de l'intelligence responsable a débuté. Ensemble, nous pouvons la construire de manière sécurisée, éthique et pour le bien commun.

Chapitre un

L'évolution des données d'entreprise

Il n'y a pas si longtemps, les données de l'entreprise étaient traitées comme un carton mis au grenier, rempli de vieux dossiers, de rapports et de documents de conformité. C'était quelque chose que l'on stockait, pas quelque chose avec lequel on vivait. Vous ne montiez au grenier que lorsque vous aviez besoin de vérifier un chiffre, de prouver quelque chose ou de satisfaire un auditeur. Mais aujourd'hui, les données vivent au rez-de-chaussée. Elles sont éveillées, câblées et gèrent l'entreprise en temps réel. Elles influencent chaque décision, gèrent chaque transaction et, si elles sont divulguées ou rendues publiques, elles peuvent révéler plus que ce que vous aviez prévu.

Mais gardez ces données privées et protégées, et elles stimuleront votre avantage concurrentiel.

L'intelligence artificielle n'existe pas en dehors des données : ce sont des données mémorisées, organisées et mises en mouvement. L'entreprise est la même maison, mais le grenier a été vidé et le cerveau se trouve bas. C'est pourquoi les lois sur la confidentialité et la sécurité qui régissent les données doivent désormais être utilisées pour régir l'IA. Alors que nous entrons dans l'ère cognitive et que l'IA se développe à un rythme plus rapide, les entreprises et les agences devront traiter les informations comme des actifs gérés tout au long de leur cycle de vie, et non plus comme des archives passives.

Ce chapitre décrit les données d'entreprise : ce qu'elles sont, comment elles sont utilisées et comment elles peuvent être optimisées à l'aide d'un moteur d'intelligence artificielle et régies par une plateforme de gestion des informations d'entreprise (GIE) dans le cloud. Nous explorerons l'IA en tant que couche intelligente du tissu informationnel de votre entreprise, intégrée aux services de contenu et aux analyses et intégrée à vos processus commerciaux opérationnels.

Le Web caché

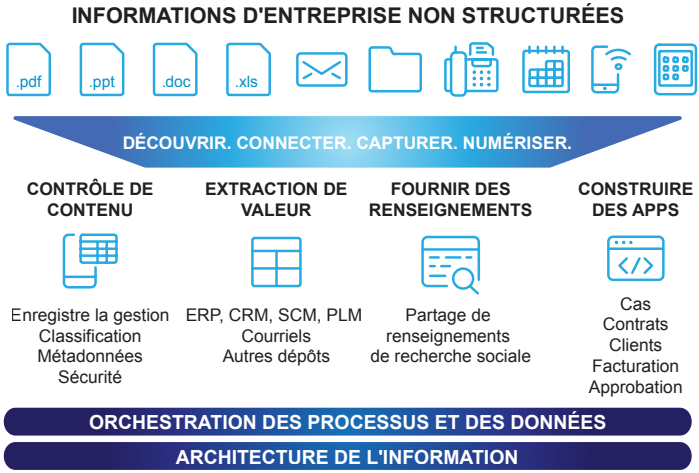
Le vrai paysage : 10 Parties privées, 1 partie publique

La plupart des informations d'entreprise les plus utiles du monde se trouvent derrière le pare-feu. IDC indique que le contenu non structuré d'une entreprise (courriels, rapports, documents, images, enregistrements) représente près de 90 % de toutes les données.[3] Ces données privées l'emportent largement sur le contenu Web public qui alimente l'IA générative d'aujourd'hui. Pourtant, une grande partie n'est toujours pas gérée, fragmentée ou piégée dans des silos.

Ce déséquilibre a de l'importance. Le ratio entre les données privées et publiques est d'environ 10 pour 1, ce qui signifie que la grande majorité du potentiel de l'intelligence mondiale est cachée aux modèles publics. Le véritable avantage concurrentiel réside au cœur de l'entreprise, sous forme de contrats, de fichiers de conception, de factures, de journaux de maintenance, de notes cliniques et de correspondance – à condition que ces informations soient gouvernées, connectées et fiables.

La gestion des informations d'entreprise a été conçue exactement pour relever ce défi. La GIE unifie, sécurise et rend opérationnelles les données de l'entreprise afin qu'elles puissent être utilisées de manière responsable et stratégique. Pour bien gérer les informations, il faut savoir où elles se trouvent, à qui elles appartiennent, qui peut les voir et quand elles changent.

Mais toutes les données ne sont pas créées de la même manière. Les données structurées, c'est-à-dire les chiffres d'une base de données, peuvent être facilement triées, interrogées et signalées. Les données non structurées (mots, images, vidéos, voix) résistent au classement. Cela nécessite de l'indexation, du contexte et de la classification. C'est pourquoi les technologies qui gèrent les nombres et celles qui gèrent les mots doivent être différentes.



Informations d'entreprise non structurées

Pour comprendre la valeur des données non structurées, considérez l'ampleur de ce qui se trouve sous chaque dossier commercial. Un employé peut apparaître sous forme de ligne dans une base de données RH, mais il est également lié à des milliers de documents : CV, contrats, fiches de paie, correspondance et évaluations de performance. Un actif, qu'il s'agisse d'un moteur d'avion ou d'une turbine, peut exister sous forme de dossier unique dans un système de planification des ressources d'entreprise (PRE), mais il est entouré d'un réseau dense de manuels, de rapports de qualité, d'inspections et de journaux de maintenance.

Ensemble, les informations structurées et non structurées forment le réseau profond ou caché de l'entreprise – des données invisibles pour les recherches publiques, mais vitales pour les opérations quotidiennes. Chaque artefact numérique contribue à cette couche cachée : chaque courriel, rapport, brouillon, image et fil de discussion. À mesure que les technologies mobiles et de collaboration se sont développées au sein de l'entreprise, la variété et la rapidité du contenu ont explosé. La GIE a évolué pour saisir, classer et gérer cette complexité, afin de s'assurer que ce qui est créé est également compris, consultable et conforme.

Mais alors que la GIE a mis de l'ordre dans les informations des entreprises, l'IA dévoile aujourd'hui sa prochaine frontière. Les modèles génératifs, principalement basés sur des données publiques, peuvent écrire, résumer et prédire, mais ils ne peuvent pas agir au cœur d'une entreprise. Ils ne disposent pas des données internes réglementées et soumises à autorisation qui permettent de prendre de véritables décisions. Sans cela, l'IA ne peut pas effectuer de tâches agentiques telles que l'approbation des factures, la planification de la maintenance ou l'interprétation de dessins techniques.

Pour franchir ce palier, l'IA a besoin de ce que la gestion de l'information offre depuis des décennies : un cadre de données d'entreprise sécurisées, conformes et autorisées. Ce n'est qu'alors qu'une IA pourra fonctionner de manière responsable à l'intérieur du pare-feu, et pas simplement imiter des intelligences provenant de l'extérieur.

Gérer ces données signifie savoir où elles se trouvent, à qui elles appartiennent, qui peut les voir et quand elles changent. Ces principes fondamentaux de la GIE, à savoir les autorisations, les métadonnées et le contrôle du cycle de vie, sont ce qui garantit la fiabilité des informations de l'entreprise. Ces fonctions doivent désormais être appliquées à l'IA.

Par où commencer ? Voyons où se trouvent les informations de l'entreprise.

Où se trouvent les données : les différents types d'informations d'entreprise

Chaque entreprise produit des informations pour plusieurs raisons : pour enregistrer ses opérations, permettre la communication, préserver les connaissances, se conformer aux réglementations et offrir de la valeur ajoutée à ses clients. Ce qui n'était au départ qu'une gestion structurée des dossiers (transactions, factures et registres d'inventaire sur ordinateur central) s'est transformé en un réseau de communication et de collaboration : courriels, documents partagés et espaces de travail numériques.

Aujourd'hui, ces flux d'informations peuvent être classés en trois grandes catégories de données d'entreprise qui revêtent une importance différente pour l'IA : les contenus générés par l'homme, les données générées par des machines et les données transactionnelles ou issues des réseaux commerciaux. Chacune a sa propre structure, ses propres exigences de gouvernance et son propre rôle dans la formation des modèles d'IA. Ensemble, ces catégories constituent la base de l'intelligence agentique au cœur de l'entreprise.

Le contenu généré par l'homme : le langage de l'entreprise

Le contenu généré par l'homme inclut des documents, des courriels, des numérisations, du contenu multimédia, des notes de cas et d'autres formes de communication. Il est riche en significations et en nuances, mais intrinsèquement non structuré. C'est le domaine de la gestion de contenu, dans lequel les informations contiennent des données personnelles, contextuelles et souvent sensibles qui nécessitent une classification minutieuse, un balisage avec des métadonnées et une gestion du cycle de vie.

Ces documents contiennent la politique, les précédents et le langage qui définissent le fonctionnement d'une entreprise. Former l'IA à ce type de contenu nécessite une anonymisation et une gouvernance rigoureuse, mais les avantages sont considérables : c'est là que résident l'intention, les règles commerciales et les connaissances institutionnelles. Lorsqu'il est correctement géré, le contenu non structuré devient la base de la génération augmentée par la recherche (GAR), des bibliothèques de messages et du raisonnement en langage naturel – des capacités qui permettent à l'IA agentique d'agir avec compréhension, et pas seulement de manière automatisée.

Les données générées par des machines : le système nerveux de l'entreprise

Les données générées par des machines proviennent des systèmes qui alimentent l'entreprise : journaux, télémétrie, indicateurs de performance et flux de surveillance. Il est riche en volume, en vitesse et en structure, et il raconte en temps réel les activités de l'entreprise. C'est le domaine de l'observabilité et de la connaissance opérationnelle, où chaque événement ou anomalie laisse une trace.

Les données des machines fournissent les signaux causaux dont l'IA a besoin pour agir intelligemment sur l'infrastructure, détecter des modèles, prédire des défaillances ou recommander des mesures correctives avant que les utilisateurs ne s'en aperçoivent. Ses défis résident dans leur ampleur, le coût de la rétention et la nécessité de mettre en correspondance les signaux bruts avec le contexte des activités. Lorsqu'elles sont associées à des politiques et à du contenu humain, ces données permettent à un agent IA de répondre de manière autonome tout en garantissant l'auditabilité et la conformité.

Les données transactionnelles et relatives aux réseaux commerciaux : la source de vérité

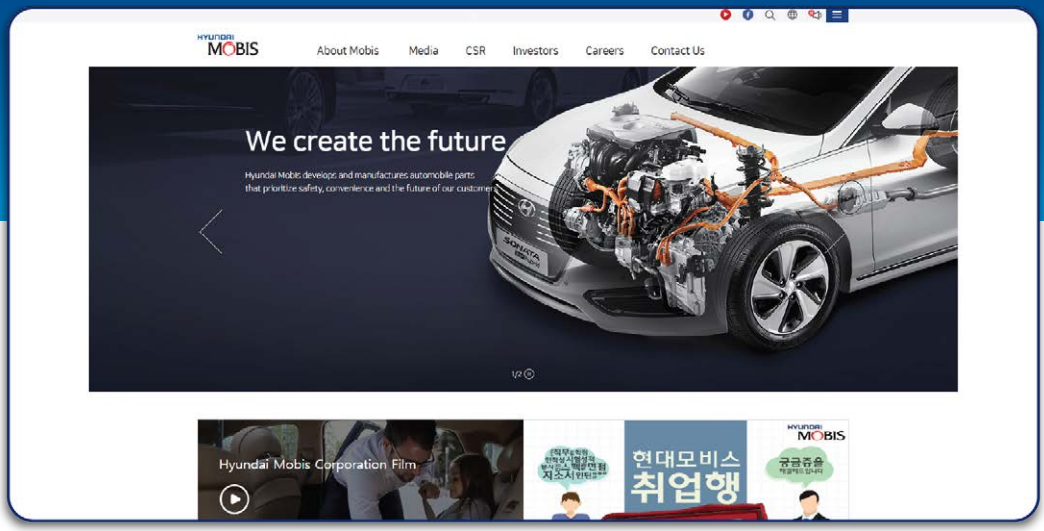
Les données transactionnelles (bons de commande, factures, avis d'expédition et autres messages structurés) représentent la vérité juridique et économique des opérations commerciales. Ces dossiers définissent les obligations entre les entreprises et sont essentiels pour la conformité, la fiscalité et l'audit. Parce qu'ils suivent des schémas bien définis et qu'ils sont d'une grande précision sémantique, ils fournissent une base fiable pour raisonner sans ambiguïté.

Pour l'IA agentique, ce sont les données transactionnelles qui ancrent les décisions dans les faits. Elles permettent aux agents de rapprocher les registres financiers, de prévoir les flux de trésorerie et d'identifier les exceptions dans les chaînes d'approvisionnement complexes sans falsifier les résultats. L'intégration de ces informations structurées aux couches non structurées et opérationnelles permet d'obtenir une vue d'ensemble de l'entreprise : ce qui se passe, pourquoi cela se passe et ce qu'il convient de faire ensuite.

Dans l'article suivant, MOBIS, un constructeur automobile, a mis en place un système de production de pièces conçu pour garantir la qualité et réaliser des économies tout au long de la chaîne d'approvisionnement, en s'appuyant sur l'analyse de données et la veille économique.

Étude de cas

MOBIS



MOBIS

Basée à Séoul, en Corée du Sud, et disposant de filiales dans environ 40 pays à travers le monde, MOBIS gère la chaîne d'approvisionnement des géants de l'industrie automobile Hyundai Motor Company et Kia Motors. L'entreprise a créé un système de production de pièces conçu pour garantir la qualité et réaliser des économies tout au long de la chaîne d'approvisionnement, des achats aux stocks en passant par les ventes et la logistique, pour aider ses clients à se démarquer dans le secteur concurrentiel de l'automobile. MOBIS Parts Australia Pty Ltd. (MPAU) est la filiale australienne du constructeur automobile.

L'industrie automobile est confrontée à des défis concurrentiels permanents, d'autres marques proposant de nouveaux produits, de nouvelles stratégies de vente et de nouvelles méthodologies de tarification. Par conséquent, MPAU doit s'assurer de disposer de systèmes et de technologies adéquats pour garantir la compétitivité de ses produits et la flexibilité de ses opérations. Afin de réagir de manière réactive à l'évolution de la demande ou aux offres de ses concurrents, l'entreprise avait besoin d'un nouveau système d'intelligence et de veille économique capable de prendre en charge la gestion des stocks en temps réel et les rapports du réseau de distributeurs, de surveiller les performances commerciales et les offres tarifaires des fournisseurs, et d'offrir des capacités d'analyse permettant de prévoir les ventes futures et les besoins en stocks.

> *Du point de vue logistique, nous sommes en mesure d'obtenir une visibilité claire sur les opérations commerciales en intégrant les informations du back-end au front-end du système d'intelligence d'entreprise, ce qui nous permet d'analyser les informations provenant du système principal.*

RESPONSABLE TI, MPAU

Après avoir testé plusieurs systèmes, MPAU a finalement choisi une suite analytique en raison de ses solides fonctionnalités et de sa facilité d'utilisation. Ce dernier élément a joué un rôle déterminant pour garantir que les utilisateurs finaux adoptent naturellement le système, afin de renforcer l'engagement des distributeurs grâce à une intégration transparente et intuitive dans les opérations quotidiennes d'environ 140 à 160 utilisateurs et revendeurs. La solution a pu s'intégrer aux sources de données des opérations de MPAU et au réseau de concessionnaires grâce à des tableaux de bord qui offraient à chaque département, des stocks à l'entreposage en passant par les ventes et la logistique, un aperçu de leurs activités quotidiennes.

Les fonctionnalités d'analytique confèrent à l'entreprise un avantage concurrentiel, en leur permettant non seulement de consulter l'historique des ventes et des stocks, mais également de prévoir les besoins futurs. Désormais, au lieu de s'appuyer sur un processus de rapports fastidieux et des prévisions imprécises, les utilisateurs peuvent comparer les données historiques aux informations commerciales actuelles en temps réel et projeter les ventes futures. Il en résulte un environnement commercial plus efficace, avec une prise de décision éclairée qui permet aux utilisateurs d'accéder aux données et d'interagir avec elles de manière plus fiable, et à l'entreprise d'opérer avec une plus grande agilité sur un marché concurrentiel.

Quand les différents types d'informations fonctionnent ensemble

Comme l'illustre l'étude de cas ci-dessus, la véritable puissance des données d'entreprise se révèle lorsque différents types d'informations convergent. Lorsque le savoir humain, la télémétrie des machines et les transactions commerciales sont régis, connectés et contextualisés, ils forment l'architecture vivante d'une entreprise intelligente.

Prenons l'exemple d'un groupe de services financiers partagés qui utilise un assistant IA pour mettre en relation des bons de commande et des factures qui ne correspondent pas. L'assistant analyse les images des factures et les sorties OCR (reconnaissance optique de caractères) – en termes plus simples, du contenu généré par l'homme) – puis les compare aux enregistrements de transactions du PRE (données transactionnelles) et passe en revue les journaux du système indiquant quand les factures ont été reçues ou approuvées (données machine). Grâce à une couche unifiée de métadonnées (qui capture la traçabilité des documents, les droits d'accès et les horodatages), l'assistant IA peut générer une recommandation justifiable qui réduit le temps de cycle et préserve l'intégrité de l'audit.

Dans un autre exemple, un agent du service juridique chargé de préparer des lettres de conservation à des fins juridiques s'appuie sur des documents stratégiques et des communications antérieures (contenu généré par l'homme), utilise des calendriers de classement et des métadonnées relatives aux dossiers (données transactionnelles) et vérifie les journaux d'accès au serveur pour confirmer la garde des données (données machine). Le résultat est un brouillon à la fois précis et conforme, produit en quelques minutes au lieu de plusieurs jours. Le même principe s'applique à grande échelle dans de vraies entreprises, comme l'illustre l'étude de cas suivante.

Étude de cas

Une entreprise énergétique indépendante

Une entreprise énergétique indépendante, qui est également un service public géré par l'État, dessert plus de 150 000 clients. L'entreprise avait besoin d'un moyen de gérer des volumes croissants d'informations tout en garantissant la conformité avec plusieurs réglementations. « En tant qu'entreprise hautement performante, nous devons nous assurer que les informations pertinentes sont disponibles au bon endroit et au bon moment afin de pouvoir prendre les bonnes décisions », explique le responsable des archives de l'entreprise. « Pour cela, nous devons intégrer des mandats de conformité, relever les défis liés à l'organisation de l'information et améliorer constamment les processus commerciaux. »

En étendant la gestion des informations d'entreprise à la recherche et à l'automatisation pilotées par l'IA, l'entreprise peut désormais localiser les informations et les exploiter plus rapidement que jamais. La récupération intelligente permet de retrouver du contenu structuré et non structuré (courriels, feuilles de calcul, rapports et PDF) au cœur d'un environnement sécurisé unique. La synthèse par IA aide les employés à interpréter de grands ensembles de données techniques et de documents réglementaires, tandis que les modèles d'apprentissage automatique signalent les problèmes de conservation et automatisent les contrôles de conformité. L'entreprise gère désormais conjointement la conformité et la performance, en utilisant l'intelligence artificielle pour rendre la gouvernance plus proactive et moins manuelle.

LA GIE et l'IA d'entreprise permettent à l'entreprise énergétique de concilier obligations réglementaires et agilité opérationnelle, transformant ainsi la gouvernance de l'information en un moteur d'analyse plutôt qu'en une contrainte. Ces exemples, qu'il s'agisse du rapprochement financier automatisé ou de la gestion de l'énergie à l'échelle de l'entreprise, illustrent la même vérité : l'IA et l'automatisation apportent de la valeur non pas à partir d'un seul ensemble de données, mais à partir des relations entre ces données. Lorsque les données sont unifiées, fiables et contextualisées, elles deviennent bien plus que de simples informations, elles deviennent de l'intelligence.

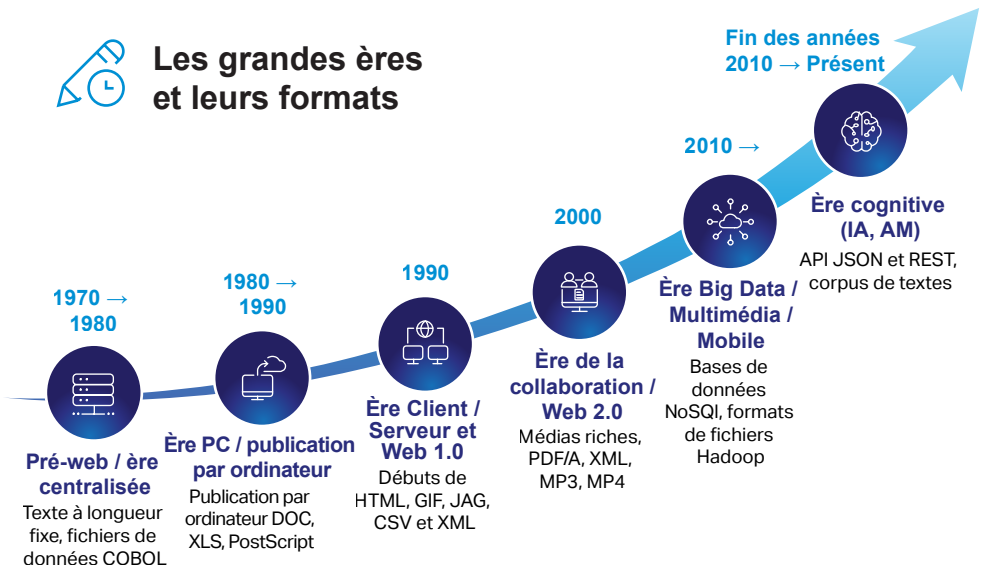
L'histoire numérique de chaque entreprise commence par ses formats. Les fichiers, les enregistrements et les conteneurs que nous utilisons pour stocker les informations reflètent les technologies et les priorités de leur époque, des cartes perforées et des fichiers d'impression aux API construites en JavaScript Object Notation (JSON) et aux ensembles de données compatibles avec l'intelligence artificielle. En examinant les cinquante dernières années d'informations d'entreprise, une vérité simple se dégage : chaque avancée dans le domaine informatique a entraîné une avancée correspondante dans le domaine du contenu.

L'ère pré-Web/Mainframe (années 1970-1980)

La première génération de données d'entreprise était stockée dans le mainframe. C'était structuré, rigide et optimisé pour l'efficacité des machines. Les enregistrements texte à largeur fixe, les fichiers de données COBOL (Common Business Oriented Language) et les formats ISAM (Indexed Sequential Access Method) indexés ont remplacé les registres manuscrits et les journaux papier. L'espace de stockage était limité, donc chaque octet comptait.

Le traitement par lots prédominait, et l'accent était mis sur le débit plutôt que sur l'interaction. Ces systèmes étaient conçus pour « traiter pendant la nuit » et produire des rapports imprimés et des fichiers spool le lendemain matin. Les schémas de codage tels que l'EBCDIC (Extended Binary Coded Decimal Interchange Code) conservaient l'aspect propriétaire et était étroitement lié au matériel qui les produisait.

Ces premiers systèmes ont jeté les bases de la discipline des données structurées. Ils ont introduit le contrôle des schémas, les formats d'enregistrement versionnés et les prémices de ce qui allait devenir les métadonnées – c'est-à-dire l'idée que chaque champ avait une signification. La rigidité du mainframe a obligé les entreprises à considérer les données comme un actif bien avant que n'existe le terme « gouvernance des données ».



Les grandes époques et les formats qu'elles ont produits

L'ère du PC et de la publication assistée par ordinateur (années 1980-1990)

L'arrivée de l'ordinateur personnel a apporté la libération et la fragmentation. Soudainement, les employés ont pu créer du contenu indépendamment de l'ordinateur central. WordPerfect et les premiers documents Microsoft Word®, les feuilles de calcul et les résultats de publication assistée par ordinateur se sont multipliés dans les bureaux et sur les disquettes.

La création d'informations est passée des centres d'entreprise aux ordinateurs de bureau individuels. Les rapports, les mémos et les présentations se sont multipliés dans de nouveaux formats numériques tels que DOC, XLS et PostScript. Pour la première fois, les documents étaient visuels, modifiables et imprimables à grande échelle.

Cette démocratisation du contenu a stimulé la productivité, mais a fragmenté le contrôle. Les données qui se trouvaient autrefois dans des systèmes centralisés étaient désormais éparpillées sur des disques durs et des partages de fichiers. Cette époque a marqué le début de « l'explosion du contenu », qui a fini par stimuler la demande de systèmes de gestion de contenu à l'échelle de l'entreprise.

Client/Serveur et Web 1.0 (années 1990)

Au fur et à mesure que les entreprises ont mis leurs systèmes en réseau, les informations ont commencé à circuler en ligne. L'essor du Web a introduit les pages HTML, les images GIF et JPG, et les premiers XML pour les échanges structurés. Les intranets internes reflétaient les sites Web publics, et le défi était passé de la création à la découverte.

Les architectures client/serveur permettaient aux employés de partager des bases de données et des applications, tandis que les navigateurs permettaient de publier des informations de manière universelle. Le besoin d'indexation et de recherche a donné naissance aux premiers modèles de métadonnées et de systèmes de gestion de documents. Cela a donné lieu à la « révolution de la recherche », caractérisée par la nécessité d'adopter une approche axée sur le cycle de vie de l'information : création, stockage, extraction et élimination.

Le Web 1.0 a transformé le savoir de l'entreprise en quelque chose de dynamique, connecté et de plus en plus complexe. Cela a également jeté les bases de la gouvernance : une fois que vous avez trouvé des données, vous devez décider qui d'autre doit y accéder.

Le Web 2.0 et l'ère de la collaboration (années 2000)

Le début des années 2000 a introduit un Web plus social et participatif. Les medias riches, les normes d'archivage PDF/A, les formats XML et JSON et les encodages multimédia tels que MP3 et MP4 sont devenus monnaie courante.

Le contenu généré par les utilisateurs et les outils de collaboration sont entrés dans l'entreprise. Les archives des courriels, les portails et les wikis ont rejoint les systèmes de dossiers traditionnels. La gestion de contenu a évolué pour prendre en charge des documents persistants et partageables qui transcendent les frontières entre les services, et même entre les entreprises.

C'est aussi à cette époque que la pression réglementaire a rejoint l'échelle numérique. La loi Sarbanes-Oxley, la loi HIPAA (Health Insurance Portability and Accountability Act) et d'autres régimes de conformité ont obligé les entreprises à prouver non seulement ce qu'elles savaient, mais aussi quand et comment elles le savaient. Cette convergence entre réglementation et collaboration a renforcé la nécessité d'une gestion des enregistrements, d'un contrôle des versions et d'un archivage basé sur des politiques, qui constituent les piliers fondamentaux de la gestion moderne de l'information d'entreprise (GIE).

L'ère des mégadonnées, du multimédia et de la téléphonie mobile (années 2010 →)

Dans les années 2010, l'information avait dépassé le cadre des documents. Les flux, les données télémétriques et les séries chronologiques provenaient d'appareils mobiles, de capteurs et d'applications. De nouveaux formats de fichiers analytiques — Avro, Parquet, ORC (Optimized Row Columnar) — optimisés pour l'évolutivité et la vitesse sont devenus la norme dans les data lakes et les entrepôts cloud.

Les référentiels de vidéos, de voix et d'images de grande taille se sont développés de façon exponentielle à mesure que les téléphones intelligents et les expériences numériques sont devenus la norme. Le stockage objet et les réseaux de diffusion de contenu ont redéfini le concept de « fichier », transformant tout en un bloc adressable avec des enveloppes de métadonnées.

Cette prolifération de données a donné naissance au « Web caché », le vaste univers de contenus non structurés cachés derrière le pare-feu. Il s'agissait à la fois d'une opportunité et d'un défi pour l'entreprise : une opportunité d'exploiter les données analytiques et d'appliquer l'apprentissage IA automatique, mais un défi en termes de coûts et de conformité.

L'ère cognitive (fin des années 2010 → aujourd'hui)

Le paysage actuel du contenu est fluide, interconnecté et multimodal. Les données circulent non seulement entre les personnes et les systèmes, mais aussi entre les machines. Les API, en particulier REST (Representational State Transfer) et GraphQL, interconnectent les microservices. Les packs spécifiques aux applications (conteneurs, carnets de notes, journaux structurés) représentent de nouveaux types de documents hybrides.

Cette ère est marquée par l'interopérabilité et l'automatisation. Les informations sont à la fois consommées et produites par l'IA, l'apprentissage automatique et les agents numériques. Les corpus de texte tokenisés, les métadonnées intégrées et le balisage sémantique permettent une génération augmentée par extraction et un raisonnement contextuel.

Alors que les époques précédentes étaient optimisées pour optimiser l'efficacité du format, l'accent est mis aujourd'hui sur le sens. L'entreprise moderne doit unifier les données structurées et non structurées quel que soit le mode (voix, image, texte et transaction) au sein d'écosystèmes gouvernés qui prennent en charge à la fois l'analytique et les actions intelligentes.

À l'ère cognitive, les formats ne sont pas statiques ; ils constituent des interfaces entre l'intention humaine et la compréhension machine. Le même cycle de vie qui s'appliquait autrefois aux documents (capture, gestion, traitement, recherche, archivage) s'étend désormais aux connaissances elles-mêmes.

À chaque époque, le thème reste le même : la technologie évolue, mais le besoin de confiance et de contexte perdure. Qu'il s'agisse de rapports COBOL ou d'API cloud, chaque nouveau format redéfinit non seulement la manière dont les données sont stockées, mais aussi la façon dont elles sont gouvernées, partagées et comprises. La leçon est simple : la gestion de l'information évolue avec le média. Ce qui a commencé comme le contrôle des fichiers est devenu le contrôle de l'intelligence. Les formats du passé étaient axés sur la lisibilité ; les formats du futur étaient axés sur l'apprentissage.

Pourquoi la gouvernance passe avant tout

La gestion des informations d'entreprise a toujours reposé sur cette confiance. Elle organise le patrimoine d'informations en termes de capture, de gestion, de traitement, de recherche et d'archivage, en liant le cycle de vie du contenu directement aux processus métier qui le créent. Quand elle est bien exécutée, la gouvernance améliore les informations, réduit les risques et diminue les coûts de mise en conformité. Ce n'est pas un ajout à la stratégie en matière d'IA ; c'est une condition préalable.

Découvrez comment UBS a centralisé ses informations sur une plateforme GIE afin de gérer ses informations et de se conformer aux réglementations dans l'étude de cas ci-dessous.

Étude de cas

UBS

Processus de certification chez UBS

En réponse aux exigences de conformité imposées par les sections 302 et 906 de la loi Sarbanes-Oxley, UBS, l'une des principales institutions financières mondiales, a mis en place un processus de certification interne des rapports financiers, dans le cadre duquel les cadres supérieurs certifient officiellement leurs chiffres et processus financiers à l'aide d'un processus de « sous-confirmation ».

Au cours du processus de certification interne, les personnes concernées sont informées par courriel lorsque leur contribution est requise, puis bénéficient d'un accès personnalisé aux documents pertinents sur l'intranet d'UBS. Tous les processus pertinents sont archivés et suivis dans un fichier journal. Le PDG et le contrôleur du groupe, généralement le directeur financier, délivrent une certification finale à la Security Exchange Commission uniquement lorsque tous les processus internes sont terminés.

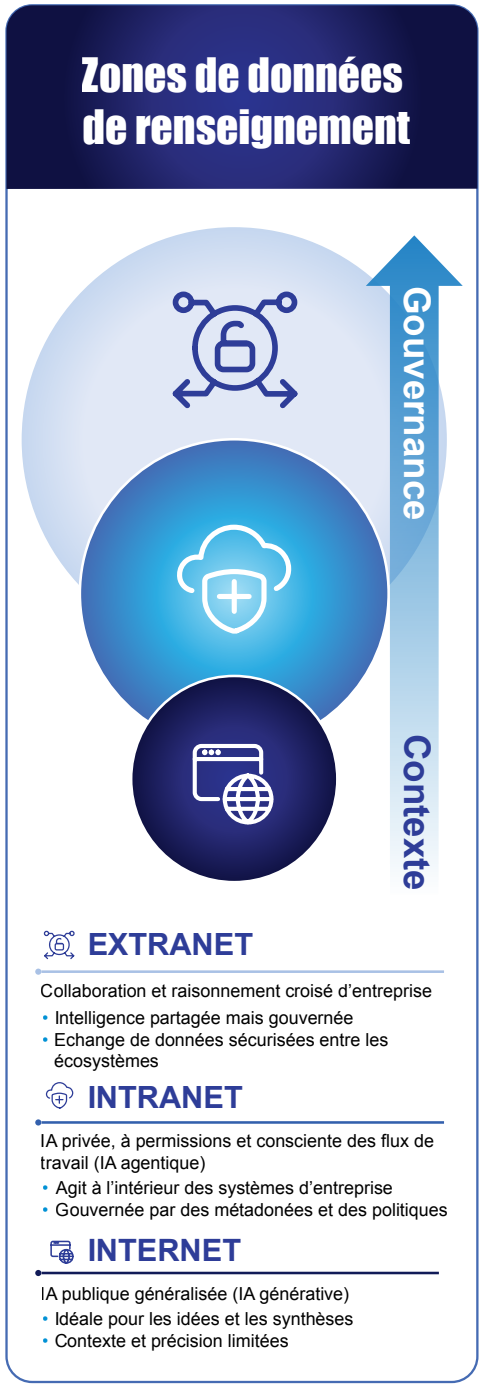
Le portail UBS sur la gouvernance d'entreprise permet aux chefs d'entreprise du monde entier de collaborer à l'élaboration de rapports commerciaux internes et externes. Les services concernés ont accès à un aperçu complet et à l'état des processus de certification à tout moment. Tous les processus connexes ont été automatisés et simplifiés, ce qui a accéléré le processus de certification.

Associer la GIE à l'IA : Internet, Intranet et Extranet

LA GIE fournit un modèle mental utile pour comprendre la maturité de l'IA. Au fur et à mesure que l'information passe du domaine public au domaine privé, l'IA passe d'une généralisation large à une intelligence contextuelle.

- **Internet = IA générative**
  La couche la plus externe représente le savoir public, c'est-à-dire les données ouvertes et les modèles linguistiques généralisés qui sont excellents pour l'idéation, les premières ébauches et l'exploration. L'IA générative fonctionne un peu comme Internet lui-même : vaste, connectée et créative, mais limitée par un manque de contexte organisationnel ou de précision.
- **Intranet = IA agentique**
  La couche intermédiaire reflète le réseau interne de l'entreprise. Ici, les données sont privées, autorisées et adaptées au flux de traitement. L'IA agentique peut raisonner sur les systèmes internes, agir sur la base de flux de traitement approuvés et prendre des décisions limitées dans le cadre des contrôles de gouvernance. C'est là que l'IA cesse de se limiter à la description et commence à agir : automatisation des tâches, renforcement du personnel et application des politiques par le biais d'actions concrètes.
- **Extranet = Intelligence artificielle générale (IAG)**
  La couche la plus interne représente la future frontière, où l'IA collabore en toute sécurité entre les entreprises et les systèmes. À la manière d'un extranet reliant des partenaires de confiance, l'IAG raisonnerait de manière fluide au-delà des frontières, en partageant des informations tout en préservant la confiance et la conformité entre les entités.

Au fur et à mesure que l'IA évolue vers l'intérieur, du public au privé en passant par les domaines partagés, son contexte, sa précision et sa valeur augmentent. Mais il en va de même pour le besoin de gouvernance. Plus le renseignement est approfondi dans les données de base de votre entreprise, plus vous avez la responsabilité de les sécuriser, de les auditer et de les aligner sur les limites humaines et réglementaires.



En chiffres : le coût énergétique de la formation d'IA

- La formation d'un modèle fondamental tel que GPT-3 a consommé environ **1287 MWh** d'électricité, émettant environ **502 tonnes métriques** de CO2, ce qui équivaut à peu près aux émissions annuelles de 112 voitures à essence.
- En 2024, une étude a révélé que jusqu'à **30 %** de l'énergie utilisée lors des cycles de formation des grands modèles linguistiques est gaspillée en raison d'une planification et d'une utilisation inefficaces du matériel, ce qui signifie que le même résultat pourrait être obtenu avec beaucoup moins d'énergie.
- Selon les projections, la demande en formation à l'IA pourrait consommer **huit térawattheures (TWh)** en 2024 et atteindre **652 TWh** d'ici 2030, ce qui représente une **augmentation de plus de 80 fois** la consommation d'électricité en seulement six ans.

Qualité des données et la physique de l'apprentissage

L'expression « à données erronées, résultats erronés » n'a jamais été aussi pertinente. La précision de tout modèle d'IA dépend de la qualité des données qu'il consomme. En termes statistiques, un plus grand nombre de données améliore les probabilités, à condition que ces données soient pertinentes, cohérentes et propres. L'apprentissage automatique moderne ne se contente pas d'ajouter du volume ; il apprend à attribuer du poids aux signaux les plus importants grâce à des entraînements et à des commentaires répétés. Au fil du temps, le système acquiert une idée de ce qui est significatif et de ce qui est du bruit, un peu comme un être humain apprend par l'expérience.

Lorsque ces entrées sont incomplètes, incohérentes ou mal gérées, le modèle comble les lacunes à lui seul. C'est là que les hallucinations se produisent : des réponses sûres, convaincantes qui sont totalement fausses. À mesure que la complexité du modèle augmente, le risque de ces erreurs augmente également. La solution réside dans la curation, c'est-à-dire l'ancrage de l'IA dans des données réglementées et hautement fiables.

Il y a également un rapport qualité/prix en jeu. Plus les données sont de qualité, moins le modèle gaspille d'énergie et de temps dans l'entraînement et l'inférence. À mesure que les modèles d'IA s'agrandissent et que les exigences informatiques augmentent, la physique de l'apprentissage devient une question d'efficacité au même titre que de précision. Des données bien organisées réduisent la redondance, minimisent le retraitement et réduisent l'empreinte de déploiement des opérations d'IA. Le nouveau chiffre du mérite réside dans l'équilibre entre la qualité des données, le temps de formation et la consommation d'énergie, ce qui nous rappelle qu'une meilleure gouvernance n'est pas seulement plus sûre, elle est aussi plus intelligente et plus durable.

Pourquoi l'IA doit suivre les règles des données

Les logiciels traditionnels traitaient les données et passaient à autre chose. L'IA ne fait pas cela. Elle se souvient. Chaque information qu'elle rencontre fait partie de son environnement interne et façonne sa façon de raisonner, de réagir et de se comporter à l'avenir. Cette mémoire différencie l'IA et rend la gouvernance essentielle.

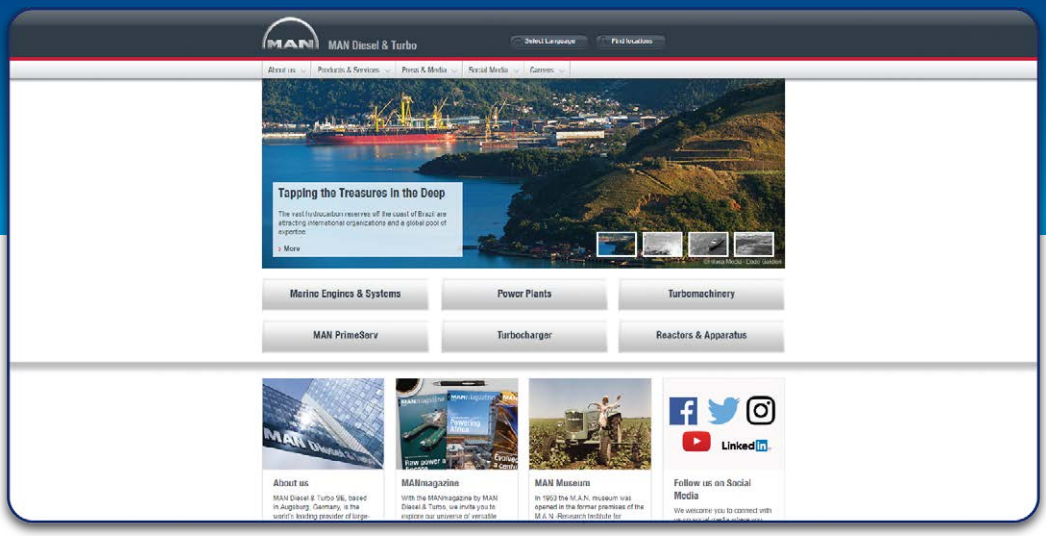
Si les données ont toujours exigé des règles, l'IA étend désormais ces règles à de nouvelles frontières. Le cycle de vie qui régit les informations de l'entreprise (capture, gestion, traitement, recherche, archivage ou élimination) doit désormais s'appliquer aux systèmes intelligents. Nous devons décider ce qu'un modèle est autorisé à apprendre, ce qu'il doit retenir, ce qu'il doit oublier et comment ses connaissances peuvent être vérifiées ou auditées au fil du temps.

Sans ces limites, la mémoire devient un handicap. L'accumulation incontrôlée transforme les informations en risques ; une gestion disciplinée du cycle de vie les transforme en informations et en valeur. La gouvernance ne se limite plus à protéger les données, il s'agit d'enseigner à l'intelligence comment se souvenir de manière responsable.

Dans l'étude de cas suivante, nous explorons comment MAN Diesel & Turbo utilise la GIE comme base de sa gouvernance et pour garantir la conformité.

Étude de cas

MAN Diesel & Turbo



MAN Diesel & Turbo

MAN Diesel & Turbo, dont le siège social est situé à Augsbourg, en Allemagne, est le premier fabricant mondial de moteurs diesel de grande cylindrée et de turbomachines. L'entreprise emploie environ 14 900 personnes sur plus de 100 sites internationaux, principalement en Allemagne, au Danemark, en France, en Suisse, en République tchèque, en Inde et en Chine.

Les moteurs diesel équipant les porte-conteneurs ou les paquebots de luxe comptent parmi les produits les plus imposants au monde et parmi ceux qui ont la plus longue durée de vie. Ils doivent fonctionner pendant des décennies et être régulièrement entretenus. En tant que l'un des principaux constructeurs mondiaux dans ce domaine, MAN Diesel & Turbo doit conserver des documents techniques importants pendant au moins 30 ans et parfois indéfiniment. L'entreprise recherchait une solution de gestion des informations pour garantir une maintenance de haute qualité et réfuter avec succès toute réclamation de responsabilité découlant de prétendus défauts de construction.

Pour garantir la conformité, MAN Diesel & Turbo s'est tournée vers les fonctionnalités de gestion des dossiers contenues dans une solution GIE étendue, ainsi que vers la gouvernance et l'archivage des applications (AGA). Les solutions combinées réunissent diverses applications afin de préserver les informations dans leur contexte. Environ 1 000 membres du personnel de service en Allemagne et au Danemark l'utilisent chaque jour pour archiver plus de 4 000 fichiers de transactions liés au processus. Dans de nombreux processus de service, les transactions sur support papier appartiennent désormais au passé, car les fichiers papier existants sont numérisés.

MAN Diesel & Turbo économise un temps précieux consacré aux recherches et à la gestion des archives papier, en plus de ses nombreuses archives numériques. La solution intégrée réduit également les besoins de maintenance en remplaçant les anciens systèmes, ce qui permet à l'entreprise de moderniser son infrastructure, de transformer numériquement les processus clés et de se conformer aux réglementations.

Le palier de l'IA en matière de données et comment le franchir

D'ici 2026, plus de 80 % des entreprises utiliseront des modèles d'IA génératifs ou des API pour la production.[4] L'ampleur de cette adoption augmente les enjeux en termes de gouvernance. Les dépenses consacrées aux outils de gouvernance de l'IA devraient plus que quadrupler d'ici 2030, les entreprises s'efforçant de gérer les risques, les autorisations, le lignage et la supervision des modèles tout en passant de l'expérimentation à l'intégration complète. [5]

L'utilisation de l'IA générative par les entreprises est désormais monnaie courante, mais une grande partie de cette activité repose toujours sur des données publiques et des modèles génériques, ce qui est excellent pour le contenu, mais limité pour l'action. En 2024, 65 % des entreprises utilisaient régulièrement l'IA générative, une part qui n'a cessé d'augmenter en 2025, mais nombre d'entre elles se contentent de « bonnes démos » plutôt que d'avoir un impact opérationnel. [6] L'écart n'est pas dû à l'enthousiasme, mais aux données. Pour fonctionner dans votre entreprise, l'IA a besoin d'un accès réglementé aux informations privées autorisées afin de pouvoir raisonner en fonction du contexte et exécuter les flux de traitement en toute sécurité.

L'expérience démontre que l'expansion sans bases solides aboutit rarement à des résultats satisfaisants. Les entreprises dotées de données fiables et de capacités d'IA surpassent régulièrement leurs pairs. [7] Ceux qui « se démarquent » le font parce qu'ils considèrent la stratégie et la gouvernance des données comme des principes fondamentaux, et non comme des considérations secondaires. Concrètement, cela implique de contrôler le contenu privé, de faire respecter les autorisations d'accès et d'appliquer des métadonnées riches en politiques afin que les modèles puissent récupérer les informations pertinentes, agir avec des garde-fous et faire preuve de responsabilité.

Lorsque l'IA fonctionne à l'intérieur du pare-feu, connectée à votre parc de données contrôlé, elle cesse de faire des suppositions et commence à travailler. Au lieu de proposer des réponses générales, elle peut prendre des mesures éclairées et responsables. Elle peut résoudre une exception de facture en se référant au bon de commande, aux conditions du fournisseur et à l'historique des approbations. Elle peut rédiger et transmettre une mise à jour de politique qui respecte automatiquement les autorisations, les calendriers de conservation et les exigences réglementaires. Elle peut répondre à une demande d'assistance en langage naturel à l'aide de connaissances approuvées et enregistrer cette interaction dans le système d'enregistrement.

Chacune de ces fonctionnalités repose sur la même infrastructure GIE qui réduit la fragmentation, régit l'accès et relie les informations non structurées aux processus métier qui en dépendent. Pour simplifier, une plateforme GIE s'occupe de l'organisation des informations. Elle régit les informations entre les systèmes, les silos et les zones géographiques. L'IA fournit du contexte. Elle tire les leçons de ces données gouvernées pour fournir des informations, de l'automatisation et de l'aide à la décision.

À l'ère cognitive, l'IA débloquera la prochaine génération de gestion de l'information. L'implication est simple : sans données privées autorisées, et sans la gouvernance nécessaire pour les utiliser de manière responsable, l'IA générative atteint un plafond. Elle peut résumer Internet, mais elle ne peut pas approuver une facture, planifier une réparation ou résoudre une exception client dans vos systèmes. La voie à suivre réside dans les données d'entreprise cataloguées, classées et soumises à un contrôle d'accès, soutenues par des pipelines vérifiables qui permettent aux agents IA d'extraire des faits, de prendre des actions définies et de laisser une trace vérifiable. C'est ainsi que les entreprises transforment l'adoption généralisée en valeur commerciale durable.

Télécharger The Fast Five

1. **La maturité de l'IA commence par la maturité des données.**
   La puissance de l'IA dépend des données dont elle tire des leçons. Les modèles génératifs basés sur des données publiques atteignent un palier – l'IA agentique nécessite des informations réglementées, privées et autorisées. Investissez dans les bases de données avant de développer les capacités de l'IA. Utilisez une GIE pour identifier les ensembles de données privés de grande valeur et appliquez l'IA lorsque la valeur du processus est claire.

2. **La gouvernance est la nouvelle infrastructure.**
   Les principes qui garantissent la conformité des données d'entreprise (métadonnées, autorisations, contrôle du cycle de vie et auditabilité) sont désormais des prérequis pour l'IA. La gouvernance définit la manière dont l'intelligence apprend, mémorise et agit en toute sécurité au cœur de votre entreprise.

3. **Déplacez-vous vers l'intérieur pour créer de la valeur : Internet → Intranet → Extranet.**
   Les données publiques alimentent l'IA générative (contenu), les données internes alimentent l'IA agentique (action), et les écosystèmes connectés alimenteront un jour une IAG (collaboration). Chaque étape augmente la précision, la responsabilité et la valeur, et exige des contrôles plus stricts.

4. **La qualité des données définit les performances de l'IA et son empreinte.**
   Des données sélectionnées et propres réduisent les erreurs, améliorent la fiabilité et réduisent le gaspillage de temps de calcul. Le nouveau chiffre de mérite équilibre la qualité, le temps de formation et la consommation d'énergie. Une meilleure gouvernance des données aujourd'hui signifie une IA plus rapide, plus écologique et plus précise dans l'avenir.

5. **L'IA doit suivre les règles des données.**
   Contrairement aux logiciels traditionnels, l'IA mémorise ce qu'elle voit. Cela fait de sa mémoire un élément de votre paysage de gouvernance. Traitez l'apprentissage de l'IA comme un cycle de vie : décidez ce que les modèles peuvent apprendre, ce qu'ils doivent retenir, ce qu'ils doivent oublier, et comment vous allez les auditer.

Chapitre deux

L'essor de l'intelligence artificielle d'entreprise

À mesure que le paysage technologique évolue, l'intelligence artificielle a le potentiel de remodeler de nombreux aspects de notre vie. Qu'il s'agisse d'améliorer la productivité sur le lieu de travail ou de révolutionner la façon dont nous interagissons avec les informations et les uns avec les autres, l'IA occupe une place essentielle dans notre vie personnelle et professionnelle.

L'intelligence artificielle d'entreprise redéfinit les performances des entreprises en transformant l'intelligence en contexte. Au fur et à mesure que l'adoption s'étend à l'expérience client, aux opérations et à la publication de contenu, le véritable avantage ne réside pas seulement dans l'automatisation, mais aussi dans la compréhension du contexte. Ce chapitre explorera les concepts clés de la technologie de l'IA, les principes fondamentaux et les applications dans différents secteurs.

> *Le nombre d'entreprises ayant entièrement modernisé leurs processus basés sur l'IA a presque doublé, passant de 9 % en 2023 à 16 % en 2024. Par rapport à leurs pairs, ces entreprises enregistrent une croissance de leur chiffre d'affaires 2,5 fois supérieure, une productivité 2,4 fois plus élevée et un succès 3,3 fois plus important dans les cas d'utilisation de l'IA générative.* [8]

L'intelligence contextuelle permet à l'IA de saisir l'intention commerciale, en interprétant non seulement les données mais aussi les structures, les flux de traitement et les objectifs qui définissent la manière dont une entreprise crée de la valeur. En cartographiant les relations entre les indicateurs, les processus et la logique métier, l'IA peut anticiper les résultats, modéliser les dépendances et recommander des actions conformes aux priorités stratégiques. Elle comble efficacement le fossé entre l'analyse et l'exécution, en transformant les informations en décisions mesurables qui stimulent la croissance, l'efficacité et la différenciation concurrentielle.

Cependant, parallèlement à ses avantages, certaines considérations et implications éthiques importantes doivent être abordées. En comprenant la double nature de l'IA – son potentiel d'innovation et sa capacité à bouleverser les choses – nous pouvons mieux nous préparer à un avenir dans lequel cette technologie jouera un rôle central. Après avoir abordé la question des données dans le premier chapitre, nous allons maintenant examiner en détail en quoi des données fiables et sécurisées constituent la pierre angulaire d'une IA efficace. Des données de qualité sont essentielles pour stimuler l'innovation tout en évitant les perturbations négatives liées à la prolifération de l'IA.

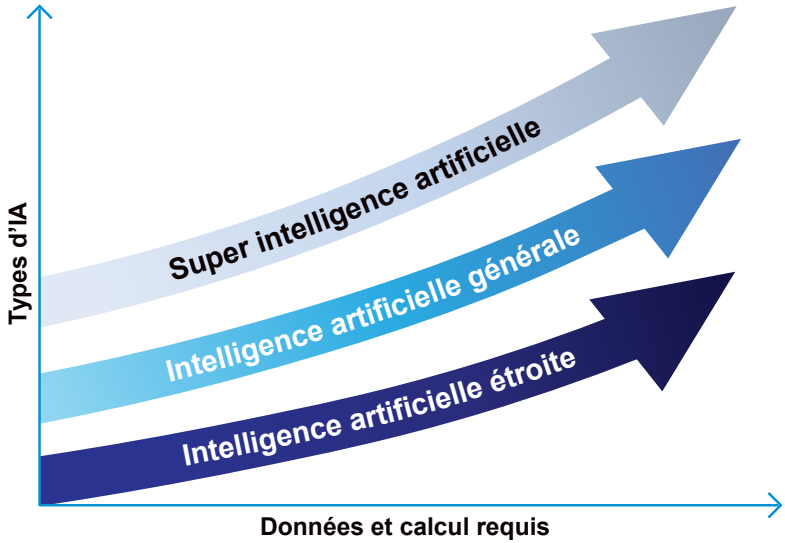
Définir l'IA

Il existe de nombreuses définitions de l'IA, mais selon l'Organisation internationale de normalisation (ISO), « l'intelligence artificielle (IA) est une branche de l'informatique qui crée des systèmes et des logiciels capables d'effectuer des tâches autrefois considérées comme exclusivement humaines. Elle permet aux machines de tirer des leçons de leur expérience, de s'adapter aux nouvelles informations et d'utiliser des données, des algorithmes et de la puissance de calcul pour interpréter des situations complexes et prendre des décisions avec un minimum d'intervention humaine. » [9]

L'IA n'est pas un concept ou une technologie unique. En fait, « l'IA est un vaste domaine comportant de nombreux sous-domaines, chacun ayant ses propres objectifs et spécifications. C'est un terme générique qui englobe de nombreuses technologies, notamment l'apprentissage automatique, l'apprentissage profond et le traitement du langage naturel (TLN). » [10]

L'intelligence artificielle se divise généralement en trois catégories : intelligence artificielle étroite, intelligence artificielle générale et intelligence artificielle supérieure. Le moyen le plus simple de comprendre les différences est de réfléchir à la façon dont chacune apprend. L'intelligence artificielle étroite est comme un étudiant qui excelle dans une seule matière. Par exemple, elle peut être excellente pour jouer aux échecs, reconnaître des visages ou prédire les habitudes de circulation, mais elle ne peut pas faire grand-chose en dehors de sa spécialité. AlphaGo de DeepMind et son successeur AlphaZero ont marqué des étapes importantes dans le domaine de l'IA en maîtrisant des jeux complexes grâce à l'auto-apprentissage et à des techniques de renforcement à grande échelle. Ils ont démontré une puissante capacité de généralisation dans des domaines restreints, tout en restant dans le domaine de l'IA étroite et non de l'IAG véritable.

L'intelligence artificielle générale (IAG), quant à elle, ressemble davantage à un étudiant diplômé aux compétences variées. L'IAG peut aborder de nouveaux sujets, échanger des idées et résoudre des problèmes dans de nombreux domaines, comme le ferait une personne. Ensuite, il y a l'intelligence artificielle supérieure (IAS), qui va encore plus loin. ASI serait une sorte de génie qui excelle dans tous les domaines : raisonnement, créativité et même amélioration de soi.



L'IA se divise en trois catégories

Le rapport *AI Watch* de la Commission européenne décrit les systèmes d'IA étroite comme des systèmes « capables d'effectuer une tâche spécifique et de fonctionner dans un environnement prédéfini. L'IA étroite peut traiter les données à grande vitesse et améliorer la productivité et l'efficacité dans de nombreuses applications pratiques. Bien que l'IA étroite soit supérieure dans les domaines spécialisés, elle est incapable de généraliser, c'est-à-dire de réutiliser ses connaissances acquises dans des domaines différents. » [11]

Le rapport explique également : « L'IAG fait référence à des machines dotées d'une intelligence humaine. En d'autres termes, l'IAG vise à accomplir toutes les tâches intellectuelles qu'un être humain peut accomplir. » [12] Nous n'en sommes pas encore au stade de l'IAG, car l'intelligence de l'IA n'est pas de nature humaine – elle est simulée. Pour atteindre pleinement l'IAG, les systèmes d'IA doivent être capables d'apprendre (en particulier, sans être ré-entraînées), de faire preuve d'autonomie et de comprendre les causes et les effets dans leur contexte.

L'IAS n'est pas encore définie dans les normes et est considérée comme un état futur au-delà de l'IAG : « L'intelligence artificielle supérieure (IAS) est un hypothétique système d'intelligence artificielle (IA) basé sur un logiciel et doté d'une capacité intellectuelle dépassant celle de l'intelligence humaine. Au niveau le plus fondamental, cette IA superintelligente possède des fonctions cognitives de pointe et des capacités de réflexion très développées, plus avancées que celles de n'importe quel être humain. » [13]

L'intelligence artificielle peut être classée de deux manières principales : par capacité (dans quelle mesure elle se rapproche de la cognition humaine) et par fonctionnalité (comment elle se comporte et interagit avec les données). Le chercheur en intelligence artificielle Arend Hintze a présenté un cadre fonctionnel largement reconnu qui explique comment les systèmes traitent les informations et réagissent à leur environnement.

Selon le cadre conceptuel de Hintze, au niveau le plus élémentaire, les machines réactives fonctionnent uniquement à partir des données du présent, sans capacité d'apprentissage à partir du passé. Le système d'échecs Deep Blue d'IBM en est un exemple bien connu. L'IA à mémoire limitée permet de conserver des données à court terme afin d'éclairer les décisions. Elle constitue la base de presque toutes les IA modernes, des véhicules autonomes aux moteurs de recommandation. Au-delà de cela, le domaine entre dans le domaine théorique : L'IA Théorie de l'esprit imagine des systèmes capables de comprendre les croyances, les émotions et les intentions humaines, tandis que l'IA consciente d'elle-même représente un stade hypothétique dans lequel les machines possèdent une véritable conscience et une perception d'elles-mêmes. Bien que ces niveaux supérieurs restent spéculatifs, comprendre ce spectre permet de déterminer où fonctionnent les systèmes d'entreprise actuels, principalement dans la catégorie de la mémoire limitée, où la valeur est créée grâce à une utilisation responsable des données, à un apprentissage régi et à un déploiement discipliné à grande échelle. [14]

Au fur et à mesure que l'IA a évolué et que différentes catégories d'IA ont été identifiées, un thème commun est apparu : les données, le calcul et la gouvernance sont au cœur des différentes variantes de l'IA. Les modèles et les capacités peuvent changer, mais la capacité à organiser, sécuriser et opérationnaliser les informations reste le principal avantage. C'est là que la gestion des informations d'entreprise sert de base à l'application de l'IA, ou intelligence artificielle d'entreprise (IAE).

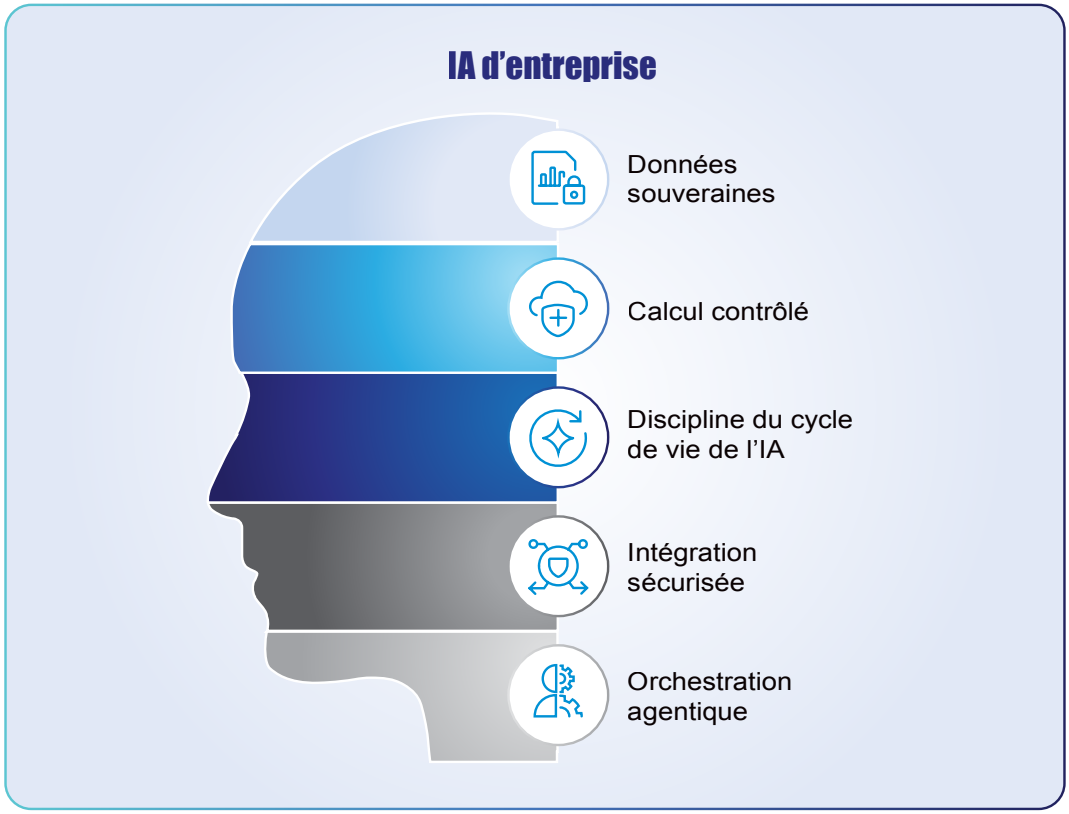
Intelligence artificielle d'entreprise

L'IA d'entreprise n'est pas une catégorie distincte d'intelligence. C'est un terme qui décrit l'application stratégique et l'intégration de différentes technologies et capacités d'IA au cœur d'une entreprise afin de résoudre des problèmes spécifiques, d'automatiser les processus et de prendre des décisions. L'IAE relève principalement de l'intelligence artificielle étroite /de l'IA faible, car les systèmes sont conçus pour effectuer des tâches spécialisées visant à améliorer les opérations, et non pour faire preuve d'une intelligence générale ou d'une conscience semblables à celles des humains.

L'IA d'entreprise repose sur :

- Des données fiables et gouvernées (la couche des « données souveraines »)
- Plateformes de gestion du cycle de vie de l'IA (par exemple, MLOps, LLMops)
- Infrastructure cloud hybride ou souveraine
- API sécurisées et couches d'orchestration
- Systèmes d'IA agentique coordonnant plusieurs modèles spécialisés

L'IA d'entreprise est une architecture gouvernée, il ne s'agit pas d'un modèle unique. Elle intègre des données souveraines, un calcul contrôlé, une discipline du cycle de vie de l'IA, une intégration sécurisée et une orchestration agentique pour fournir une automatisation fiable à grande échelle. Il s'agit d'un contexte de déploiement permettant de mettre en œuvre des technologies et des capacités d'IA éprouvées.



IA d'entreprise

Pour apporter de la valeur, les solutions IAE s'appuient sur une vaste boîte à outils :

- **L'apprentissage automatique** permet des analyses prédictives, avec la capacité d'anticiper les pannes d'équipement, de prévoir la demande ou d'optimiser les stocks.
- **Le traitement du langage naturel (NLP)** alimente les chatbots intelligents, la synthèse de documents, et analyse du sentiment des clients.
- **La vision par ordinateur permet une** automatisation qui peut être utilisée pour les inspections de fabrication et pour améliorer la surveillance de la sûreté et de la sécurité.
- **L'automatisation robotique des processus (RPA)** rationalise les tâches structurées et répétitives telles que la saisie de données et le rapprochement des factures. Et l'IA générative soutient de plus en plus la création de contenu, la génération de code et l'assistance aux connaissances.

Ce qui différencie l'IA d'entreprise, ce n'est pas le type de modèle sous-jacent, mais l'intégration contrôlée de ces technologies dans les flux de travail, les systèmes de données et les processus décisionnels de l'entreprise. Le succès ne vient pas de modèles isolés, mais de leur orchestration responsable à grande échelle, sur la base de données fiables, d'une infrastructure sécurisée et d'une solide gouvernance de l'information. L'IA d'entreprise est fondamentalement différente de l'IA destinée au grand public, tant en termes d'objectif que de conception. L'IA grand public vise à améliorer les expériences individuelles, en recommandant des films, en les aidant à effectuer des tâches personnelles ou en activant des assistants virtuels. Ces systèmes fonctionnent généralement à petite échelle, s'appuient sur des données accessibles publiquement ou fournies par les utilisateurs, et nécessitent une intégration limitée avec d'autres outils. Leur valeur réside dans la commodité et la personnalisation pour un seul utilisateur.

En revanche, l'IAE est conçue pour être évolutive, sûre et avoir un impact stratégique. Elle fonctionne sur des données commerciales sensibles et exclusives stockées dans des dossiers CRM, des systèmes PRE et d'autres bases de données opérationnelles et elle doit respecter des exigences strictes en matière de gouvernance, de conformité et de cybersécurité. L'IA d'entreprise s'intègre parfaitement aux systèmes et flux de traitement existants, automatise les processus interservices complexes et fournit des résultats mesurables tels que l'efficacité opérationnelle, la réduction des risques, les économies de coûts et l'innovation. L'IA d'entreprise est essentiellement l'application industrielle des technologies modernes d'IA, conçue pour fonctionner dans de vastes environnements où la précision, la responsabilité et la confiance sont aussi importantes que le renseignement lui-même.

Découvrez comment un aéroport international utilise l'IA d'entreprise pour permettre à plus de 90 millions de passagers de se déplacer facilement à travers le monde dans l'étude de cas suivante.

Étude de cas

Un aéroport international

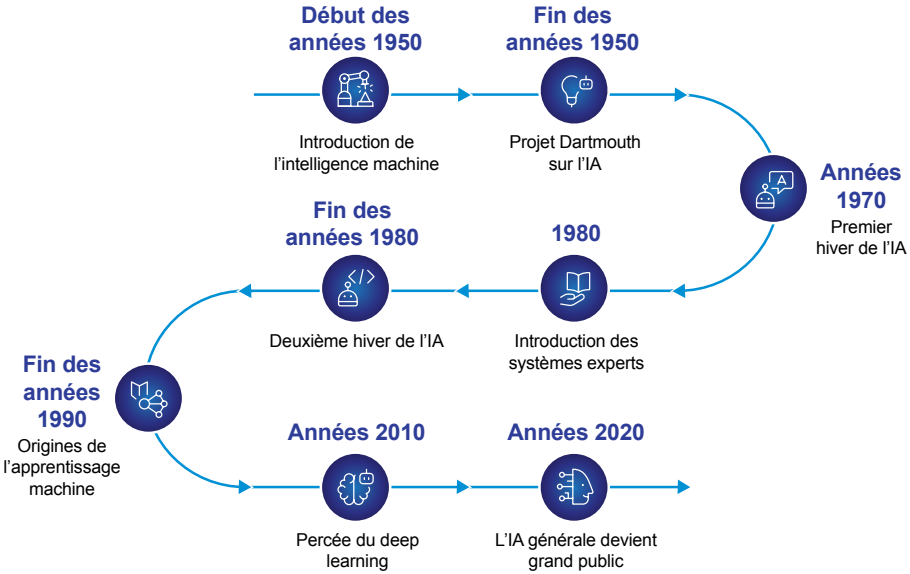
> *La plupart de nos données étaient cloisonnées entre plusieurs systèmes, et garantir leur exactitude, en particulier pour le suivi des flux de passagers et des temps de traitement, a représenté un véritable défi. Le personnel manquait souvent d'informations en temps réel ou d'outils prédictifs pour gérer de manière proactive les files d'attente, l'affectation du personnel et la congestion.*

Responsable de la gestion des services informatiques de l'aéroport

Desservant plus de 90 millions de voyageurs par an, cet aéroport est l'un des plus fréquentés au monde en termes de trafic international de passagers, et l'un des plus avancés sur le plan numérique. Il se distingue en tant que plaque tournante mondiale connue pour son innovation, son efficacité et son service client exceptionnel. Depuis son ouverture en 1960, l'aéroport s'est considérablement développé, ajoutant de nouvelles pistes, de nouveaux terminaux et de nouveaux halls pour faire face à l'augmentation du trafic aérien.

Poser les bases numériques de cette croissance n'a pas été facile. La communication est complexe entre des parties prenantes telles que les compagnies aériennes, la police, les douanes et les prestataires de services. Tout le monde doit avoir accès aux mêmes données pour prendre des décisions coordonnées. Dans le cadre d'une vaste initiative de gestion des services, l'aéroport s'est associé à un fournisseur de technologie pour étendre ses capacités de surveillance. Un composant de gestion des opérations basé sur l'IA fournit une surveillance et une gestion centralisées et intelligentes dans des environnements informatiques complexes. Il améliore l'observabilité, réduit le bruit des alertes, prédit les problèmes et contribue à maintenir le temps de service.

Les informations en temps réel et la surveillance intelligente ont transformé l'informatique, qui est passée d'une fonction dorsale à un moteur essentiel de la qualité du service, de la confiance des parties prenantes et de la satisfaction des clients, avec des impacts mesurables. En utilisant l'IA en complément d'une infrastructure GIE, l'aéroport a été en mesure de prévenir 30 % des incidents grâce à une surveillance proactive, de mieux adapter les opérations informatiques aux besoins commerciaux et de renforcer le service client grâce à l'excellence de ses systèmes informatiques.



L'évolution de l'IA moderne

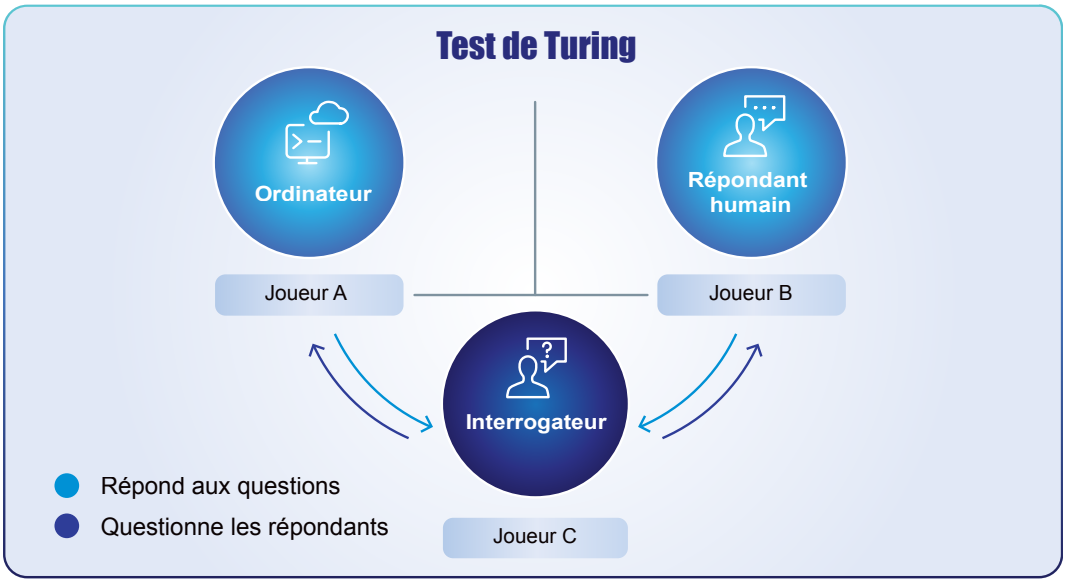
Au cours des 75 dernières années, l'IA a évolué pour devenir ce que nous connaissons aujourd'hui, certaines années étant marquées par d'incroyables innovations, d'autres par un engouement pour le développement de cette technologie. Remontons le temps pour comprendre comment nous en sommes arrivés là.

Début des années 1950 : Alors que l'intelligence artificielle a évolué au fil des décennies, Alan Turing est considéré comme l'un des premiers innovateurs. Dans son article de journal de 1950 intitulé « Computing Machinery and Intelligence », il a suggéré que les machines pouvaient simuler le raisonnement humain et a introduit le test de Turing pour l'intelligence artificielle. [15]

Fin 1950 : Avance rapide jusqu'en 1956, date à laquelle le terme « intelligence artificielle » a été introduit dans le cadre du projet de recherche estival sur l'intelligence artificielle de Dartmouth. Cette conférence, organisée par John McCarthy, Marvin Minsky, Nathaniel Rochester et Claude Shannon, est considérée comme le point de départ de l'intelligence artificielle en tant que sujet de recherche. Cet événement a réuni des chercheurs afin de formaliser l'objectif de créer des machines capables de raisonner et d'apprendre comme les humains. [16]

Années 1970 : Cependant, l'enthousiasme suscité par la conférence n'a pas duré longtemps. Bien que les recherches aient lentement progressé, la réalité de l'IA n'a pas répondu aux attentes et les premiers projets se sont révélés infructueux. Le terme « hiver de l'IA » a été formulé pour décrire une période pendant laquelle les critiques concernant l'absence de progrès, notamment le rapport Lighthill publié au Royaume-Uni en 1973, ont entraîné la suppression du financement public. [17]

Années 1980 : Après l'hiver de l'IA des années 1970, la recherche sur l'IA a connu un second souffle dans les années 1980 avec l'essor des systèmes experts et des programmes basés sur des règles du « si-alors », conçus pour imiter le comportement humain. Ces systèmes ont commencé à apparaître partout et, pour la première fois, les entreprises ont commencé à percevoir une véritable valeur commerciale dans l'IA. Cette application de l'IA était limitée et spécifique à des tâches uniques, loin d'être comparable à une véritable intelligence générale. [18]



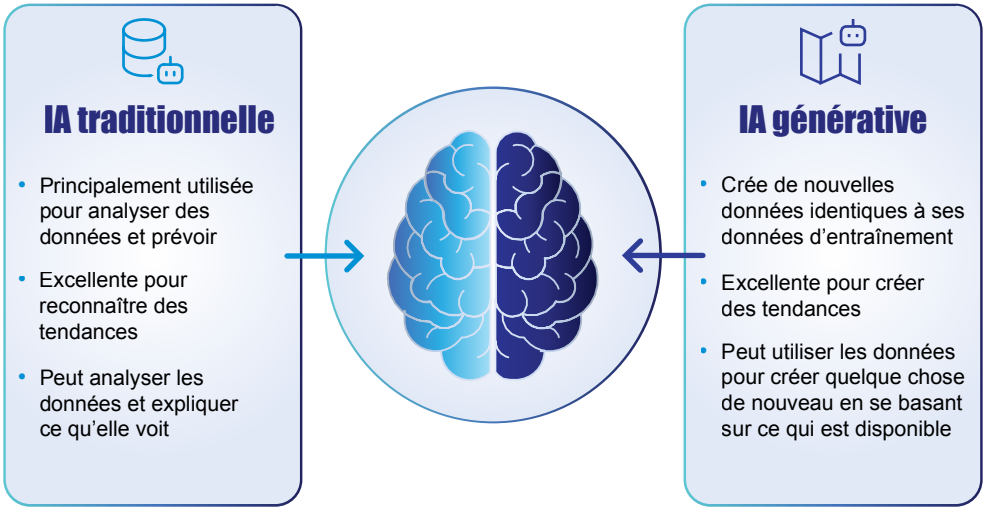
Le test de Turing

Fin des années 1980/début des années 1990 : Mais alors que les choses s'annonçaient positives, il y a eu un deuxième hiver sur l'IA. À la fin des années 1980, l'enthousiasme s'est estompé lorsque les entreprises ont constaté que ces programmes étaient coûteux à développer et à entretenir. Les limites de la logique programmée sont également devenues évidentes. À mesure que les financements se sont taris, l'IA a connu un nouveau ralentissement. [19]

Fin des années 1990 : Bien que l'IA ait connu une période de ralentissement, les recherches ne se sont pas arrêtées. Les chercheurs ont travaillé sur différentes approches, en s'éloignant des modèles « si-alors » codés en dur pour rechercher des méthodes permettant aux machines d'apprendre à partir des données. C'était l'essor de l'apprentissage automatique moderne. Parmi les avancées des années 1990, citons les algorithmes pour les réseaux neuronaux et les arbres de décision. C'est également à ce moment-là que l'apprentissage à partir des données est devenu un facteur essentiel de l'évolution de l'IA. [20]

Années 2010 : Une autre avancée a eu lieu en 2012 avec l'avènement du Deep Learning (Apprentissage profond). Cela s'est produit lorsqu'un réseau neuronal appelé AlexNet a dominé la compétition ImageNet dans le domaine de la reconnaissance d'images, en réduisant considérablement les taux d'erreur. Il s'agissait d'une avancée majeure pour la recherche, car cela démontrait que l'IA pouvait surpasser les humains en matière de reconnaissance visuelle. Google, Facebook, puis OpenAI ont poursuivi sur cette lancée en développant des systèmes d'IA capables non seulement de reconnaître des images, mais également de traduire des langues et de générer du texte. [21]

Années 2020 : Aujourd'hui, l'IA générative (GenAI) est devenue courante. Les modèles linguistiques étendus (MLE) comme GPT, Claude et Gemini arrivent à maturité et améliorent les capacités de l'IA. On s'est également rendu compte que la taille des modèles, les données utilisées pour la formation et la puissance de calcul disponible sont cruciales pour les performances. Grâce à ces innovations, les consommateurs peuvent acquérir une expérience pratique de l'IA, ce qui permet de l'adopter rapidement dans la vie de tous les jours. L'IA d'entreprise est également en train de devenir un facteur de différenciation en termes de performances commerciales.



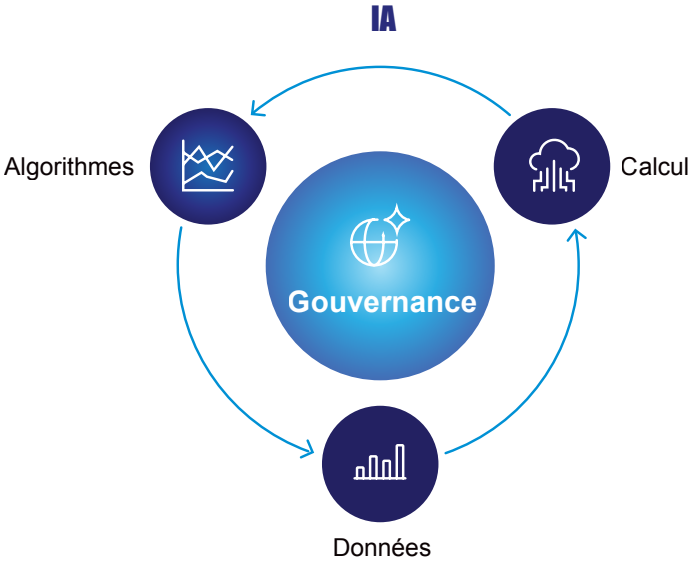
Les différences entre l'IA traditionnelle et l'IA générative [22]

Les données, le calcul, les algorithmes et la gouvernance sont au cœur du moteur de l'intelligence artificielle d'entreprise moderne

L'intelligence artificielle dans les années 2020 a progressé grâce à la convergence de trois forces : les données, la puissance de calcul et les algorithmes, qui fonctionnent ensemble dans le cadre d'une gouvernance rigoureuse. Les données fournissent le carburant essentiel, la matière première qui permet aux systèmes d'IA d'apprendre, de s'adapter et de généraliser à travers les domaines. La qualité, l'étiquetage et l'intégration de ces données déterminent l'efficacité des modèles : des ensembles de données diversifiés et bien gérés produisent des résultats plus précis et plus résilients.

La puissance de calcul permet d'évoluer. Les avancées matérielles, en particulier les unités de traitement graphique (GPU), les unités de traitement tensoriel (TPU) et l'infrastructure élastique basée sur le cloud, ont permis d'entraîner des modèles d'une ampleur inimaginable il y a dix ans.

Dans le même temps, l'innovation algorithmique s'est accélérée, donnant naissance à des modèles fondamentaux qui soutiennent l'IA générative et les systèmes d'IA multimodaux actuels. Ensemble, ces trois éléments (données, calcul et algorithmes) constituent le cœur technique de l'IA moderne. Mais la gouvernance fournit la couche d'intégrité qui garantit que chacun fonctionne de manière responsable. Quand ces forces agissent de concert, les entreprises gagnent non seulement en raisonnement et en créativité, mais aussi en confiance, en conformité et en performance durable.



IA = La combinaison de données, de calculs et d'algorithmes

Comme l'histoire l'a démontré, l'évolution de l'intelligence artificielle a rarement suivi une trajectoire rectiligne. Les progrès se sont déroulés selon des cycles familiers d'optimisme et de correction, chaque vague d'innovation étant suivie d'une période de recalibrage. Les premières percées ont souvent suscité des attentes démesurées, qui ont cédé la place à la désillusion lorsque les résultats n'ont pas été à la hauteur. Ces cycles ont pourtant été essentiels à la maturation du domaine, obligeant les chercheurs et les entreprises à trouver un équilibre entre ambition et réalisme.

Au fil du temps, un constat est resté inchangé : la viabilité de la capacité d'IA de l'entreprise dépend de l'équilibre. Les véritables progrès découlent de la synergie entre trois piliers interdépendants : des données bien gérées, des calculs évolutifs et efficaces, et des algorithmes en constante amélioration. Les entreprises qui alignent ces éléments dans un cadre de gouvernance solide sont celles qui transforment l'expérimentation en valeur commerciale mesurable.

Dans l'étude de cas suivante, une société de recherche médicale utilise l'IA d'entreprise pour connecter les données cliniques, financières et les résultats des patients à travers le pays, fournissant une analyse holistique pour aider une transformation des soins de santé basée sur la valeur.

Étude de cas

Une plateforme de soins de santé à l'échelle nationale

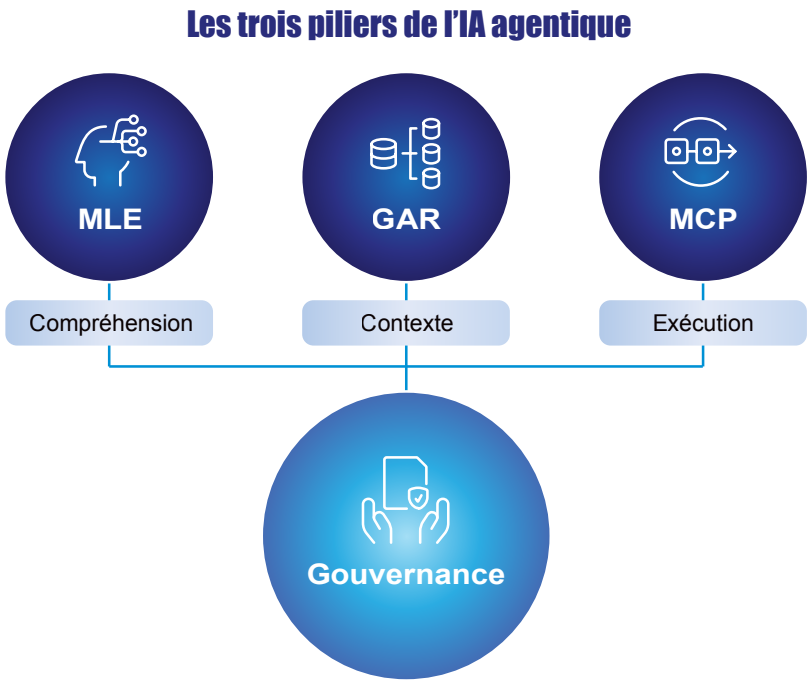
Dans le cadre d'une réglementation stricte en matière de confidentialité des données, une société néerlandaise de recherche médicale permet à ses utilisateurs (hôpitaux, gouvernement, entreprises pharmaceutiques et compagnies d'assurance) de comparer leurs performances, les expériences et les résultats des patients entre les hôpitaux et les cliniciens. Elle aide continuellement les professionnels de santé à fournir des soins de santé basés sur la valeur, en utilisant à la fois des données cliniques, financières et de mesure des résultats des patients. L'entreprise avait besoin d'une solution capable de fournir un tableau de bord en ligne intuitive, avec des capacités de scalabilité. Ils ont opté pour une combinaison d'IA et de rapports d'intelligence commerciale (IC).

Plus de 5 000 utilisateurs accèdent régulièrement à la solution pour évaluer les performances et faire des comparaisons avec leurs pairs. À l'aide d'un tableau de bord d'analyse détaillé, ils peuvent accéder aux détails des indicateurs de haut niveau. En ayant un accès facile à ces informations analytiques, les cliniciens ont pu identifier les domaines qui fonctionnent bien et ceux qui nécessitent un examen plus approfondi. Ils peuvent ensuite appliquer les améliorations appropriées si nécessaire. Par exemple, l'utilisation de cette solution a permis de réduire les complications après une chirurgie du cancer du côlon de plus de la moitié en quatre ans.

Tous les hôpitaux des Pays-Bas utilisent désormais la solution, et il est prévu d'inclure d'autres secteurs cliniques. L'étendue des possibilités offertes par l'IA ne fait que commencer à se manifester. D'autres domaines, tels que l'aide à la décision où les patients et les cliniciens peuvent choisir ensemble le traitement optimal, constituent un cas d'utilisation intéressant pour cette entreprise de recherche médicale.

Le rôle croissant des agents IA

Les agents IA passent rapidement du stade de concept à celui de fonctionnalité de base. Dans tous les secteurs, ils redéfinissent la façon dont le travail est effectué, en automatisant ce qui est répétitif, en accélérant ce qui est stratégique et en amplifiant l'expertise humaine. Dans le domaine du service client, les agents surveillent désormais les comportements, signalent les risques de désabonnement et déclenchent des campagnes de fidélisation avant même qu'un ticket d'assistance ne soit déposé. Dans le domaine des ventes, ils identifient les prospects, automatisent les suivis et fournissent des informations en temps réel qui permettent de conclure des contrats plus rapidement. Les équipes marketing utilisent l'IA pour optimiser la segmentation et personnaliser les campagnes à grande échelle. Pendant le développement de produits, les agents intelligents passent au crible les commentaires, évaluent et comparent avec les concurrents et accélèrent les décisions relatives aux stratégies. Chaque fois que les données se reproduisent, l'IA intervient, non pas pour remplacer les individus, mais pour étendre la portée de leurs capacités.



Les trois piliers de l'IA agentique d'entreprise

Les **modèles linguistiques étendus (MLE)** sont des algorithmes qui excellent lorsqu'il s'agit de comprendre le langage naturel, de récupérer des informations et de fournir des réponses claires et conversationnelles. Mais pour exécuter de véritables tâches (configurer des campagnes marketing, créer des parcours utilisateurs ou tester des modèles de tarification), il faut du contexte : une compréhension du fonctionnement réel des systèmes d'entreprise. C'est là que les architectures GAR (génération augmentée par la recherche) et Modèle Contexte Protocole (MCP) redéfinissent les limites des capacités.

La génération augmentée par la recherche (GAR) est un processus qui renforce les performances MLE en injectant des connaissances pertinentes et spécifiques au domaine dans chaque réponse. La documentation propriétaire, les référentiels de code et les instructions de processus, intégrés de manière sécurisée via GAR, permettent à un MLE d'accéder au « comment » de la tâche. Plutôt que de s'appuyer uniquement sur des données publiques, il s'appuie sur la base de connaissances réglementée de l'entreprise pour générer des conseils précis et conformes.

Le serveur MCP (Modèle Contexte Protocole) termine la boucle. En tant que couche de communication, un serveur MCP fait le lien entre l'IA générative et les systèmes, les bases de données et l'API de l'entreprise. Cela permet à l'IA de passer de la conversation à l'action, en récupérant des données, en effectuant des transactions ou en déclenchant des flux de traitement en temps réel. Les environnements logiciels modernes peuvent comprendre des centaines de points d'extrémité MCP, chacun permettant à l'IA d'exécuter une opération spécifique sous le contrôle de politiques.

Ensemble, ces trois piliers (MLE, GAR et MCP) constituent la base de l'IA agentique dans l'entreprise. Ils transforment le langage en logique, l'intention en exécution et les informations en résultats mesurables. Il s'agit de la prochaine évolution des systèmes intelligents : gouvernés, contextuels et capables de travailler aux côtés de l'homme pour favoriser la transformation dans toutes les fonctions.

C'est exactement ce qu'a fait une société minière internationale en accélérant le calendrier de ses projets de recherche grâce à l'IA, dans l'étude de cas ci-dessous.

Étude de cas

Une société minière internationale

Cette société minière internationale, dont le siège est au Brésil, produit du fer, du nickel, du cuivre, du manganèse, etc. L'entreprise mène des recherches soigneuses pour évaluer à la fois la viabilité et les impacts sociaux et environnementaux de ses activités minières. Leurs projets de recherche peuvent prendre jusqu'à dix ans. En général, les équipes interfonctionnelles passent des semaines ou des mois à collecter et à consolider manuellement les informations à examiner au fur et à mesure que de nouvelles opportunités de produits, des fluctuations du marché ou des normes environnementales apparaissent. Les projets de recherche de la société minière ont été entravés par un travail manuel de mauvaise qualité et par un assistant IA inadéquat qui manquait d'évolutivité pour une portée mondiale.

Forte d'une longue tradition d'innovation technologique pour soutenir ses activités, l'entreprise a cherché une solution qui pourrait aider ses spécialistes à réduire les tâches manuelles répétitives, accélérant ainsi la phase de recherche, tant pour les nouvelles mines que pour les mines existantes. Un porte-parole de cette société minière mondiale a déclaré : « Les informations relatives à chaque projet minier sont généralement stockées dans différents formats sur des systèmes cloisonnés et y accéder prend un temps précieux, car les travailleurs parcourent des montagnes de documents. Une IA, capable d'ingérer et d'analyser rapidement de gros volumes de données, était l'occasion idéale de réduire ce travail manuel. »

La société minière a construit une preuve de concept avec un prestataire d'IA et, grâce à une formation experte et en appliquant les meilleures pratiques, elle a pu augmenter la précision des réponses de son IA de 47 %. En utilisant l'IA pour effectuer des recherches sur des projets miniers, l'entreprise a réduit le nombre de mois de travail manuel subalterne et a stimulé une croissance rapide. S'ils ont besoin d'évaluer la faisabilité d'utiliser une mine existante pour produire du minerai, par exemple, ce qu'un géologue pourrait terminer en deux mois, les informations pertinentes peuvent être consolidées en quelques heures, ce qui aidera l'entreprise à saisir rapidement des opportunités d'investissement viables et à garder une longueur d'avance sur les évolutions du marché.

La voie à suivre pour l'IA

Si l'on repense aux 75 dernières années d'intelligence artificielle, une leçon claire s'impose : le véritable succès de l'IA n'a jamais été uniquement une question de technologie. Bien que les avancées en matière de données, de calcul et d'algorithmes aient permis des progrès remarquables, l'impact le plus durable est dû à l'alignement de ces avancées sur une gouvernance solide, des principes éthiques et une collaboration humaine.

L'IA d'entreprise représente bien plus que la prochaine phase de l'intelligence artificielle : elle marque une refonte fondamentale de la façon dont les gens interagissent avec la technologie. Contrairement à l'IA générative traditionnelle, qui produit des résultats en réponse à des instructions, les systèmes agentiques font preuve d'autonomie, d'initiative et de raisonnement adaptatif. Ils peuvent planifier, agir et apprendre dans des contextes réels, en passant de la conversation à l'exécution sans aucune direction humaine constante.

Ce changement marque le retrait discret de l'interface utilisateur graphique (GUI) en tant que modèle d'interaction dominant. Les boutons, onglets et menus de l'ère des interfaces graphiques cèdent la place à une collaboration directe avec des agents intelligents par le biais du langage naturel et de la voix. Au lieu de naviguer dans le logiciel, les utilisateurs expriment désormais leur intention, et le système interprète, décide et agit.

Le résultat n'est pas la disparition de l'interface, mais son évolution. La surface visible des logiciels s'estompe, et il ne reste que des informations qui opèrent par le biais de la conversation, du contexte et de la confiance. Dans ce nouveau paradigme, la productivité n'est plus mesurée en termes de clics par minute, mais en fonction de la qualité des résultats obtenus grâce au partenariat homme-IA.

L'intelligence agentique est déjà en train de remodeler la façon dont les entreprises produisent, gèrent et personnalisent le contenu. Les cycles de recherche sont automatisés, les premières ébauches sont générées et les expériences sont organisées en temps réel, en fonction du comportement et des préférences du public. L'IA ne se contente pas de réagir, elle raisonne en prédisant l'impact de chaque changement en aval. Pour les entreprises, l'opportunité est claire : l'intelligence contextuelle ne remplace pas le jugement humain : elle l'amplifie en développant l'expertise, la gouvernance et la créativité au cœur de l'entreprise.

Dans le futur, la prochaine ère de l'IA sera définie non seulement par un pouvoir accru, mais aussi par une autonomie, une transparence et une responsabilité accrues. Elle sera définie par des systèmes capables d'agir intelligemment tout en restant explicables et conformes aux valeurs humaines. Comprendre ce qu'est l'IA, d'où elle vient, comment elle fonctionne et à quel moment les principales étapes sont survenues constitue la base d'un leadership réfléchi qui façonnera l'avenir.

Dans ce contexte, le chapitre suivant explore l'intersection des données et de l'IA, en examinant comment la fusion de l'information et de l'intelligence crée de nouvelles possibilités d'innovation, de confiance et de profit dans l'entreprise moderne.

Télécharger The Fast Five

1. **L'IA est vaste, évolutive et fondatrice.**
   L'intelligence artificielle d'entreprise n'est pas une technologie unique mais un terme générique qui couvre divers sous-domaines tels que l'apprentissage automatique, l'apprentissage profond et le traitement du langage naturel. Cela va des systèmes restreints spécifiques aux tâches (IA étoite) à l'objectif conceptuel des systèmes superintelligents (ASI). Comprendre ces distinctions est essentiel pour prendre des décisions éclairées.

2. **La qualité des données et la gouvernance sont essentielles.**
   L'efficacité et la fiabilité de l'IA dépendent de données de haute qualité et bien gérées. Les données sont le « moteur » de l'innovation en matière d'IA ; sans données fiables, sécurisées et bien gérées, les systèmes d'IA sont sujets à des erreurs, à des biais et à des risques opérationnels.

3. **Le progrès technologique suit les cycles du battage médiatique.**
   L'histoire de l'IA est marquée par des cycles d'innovation rapide et par des périodes de désillusion (hivers liés à l'IA). Ces cycles ont fait mûrir le terrain, mettant en évidence le fait que la valeur durable repose sur un équilibre entre les avancées technologiques, des attentes réalistes et des investissements prudents.

4. **La puissance de calcul et les algorithmes avancés sont à la base de l'IA moderne.**
   Les avancées en matière de matériel (GPU, TPU, infrastructure cloud) et de conception d'algorithmes ont permis de créer les systèmes actuels d'IA générative à grande échelle. La synergie entre les données, le calcul et les algorithmes est ce qui distingue les leaders dans le domaine de l'IA.

5. **La gouvernance, l'éthique et l'alignement humain sont essentiels pour l'avenir.**
   La prochaine ère de l'IA sera définie par des systèmes qui seront non seulement puissants, mais aussi transparents, explicables et conformes aux valeurs humaines. Le succès nécessitera une gouvernance solide, des cadres éthiques et une supervision humaine pour garantir que l'IA améliore la valeur commerciale tout en renforçant la confiance.

Chapitre trois

L'intersection des données et de l'intelligence artificielle

Dans ce chapitre, nous explorons l'intersection des données et de l'intelligence artificielle, en nous concentrant sur la façon dont les informations deviennent de l'intelligence.

En nous appuyant sur les bases énoncées aux chapitres 1 (Données) et 2 (IA), nous examinons comment les données et les renseignements forment une chaîne de valeur continue. Les données alimentent le moteur de l'IA ; l'IA, en retour, dévoile la valeur latente des données. L'apprentissage continu permet de boucler la boucle et d'améliorer la précision, l'adaptabilité et la perspicacité au fil du temps. La gouvernance relie ces deux mondes, garantissant qu'au fur et à mesure que l'intelligence de l'entreprise se développe, elle reste explicable, vérifiable et alignée sur la confiance de l'entreprise. Enfin, nous examinerons les implications stratégiques et économiques de la combinaison des données et de l'IA.

Là où les données et l'intelligence se rencontrent

Dans le chapitre 1, nous avons retracé l'évolution des données : comment elles sont devenues le fondement de la gestion des informations d'entreprise et comment leur structure, leur gestion et leur accessibilité génèrent de la valeur commerciale. Le chapitre 2 a examiné de plus près l'intelligence artificielle en tant que moteur de l'automatisation et de l'intelligence, en retraçant son évolution technologique au-delà du cycle de battage médiatique vers le déploiement de l'IA agentique dans le monde réel.

Tout au long de ce livre, notre thèse centrale est que les données et l'IA sont symbiotiques. Les données fournissent à l'IA le contexte et le potentiel nécessaires pour apprendre, tandis que l'IA transforme les données en informations exploitables. Ensemble, elles stimulent l'innovation dans les entreprises modernes.

L'IA performante nécessite des données de haute qualité. Il s'agit de données bien gouvernées, structurées, contextuelles et sécurisées. Les données ne sont pas toutes créées de la même manière. Les différents ensembles de données ont des exigences différentes, en particulier lorsque les entreprises tentent d'équilibrer les données publiques et privées. Les ensembles de données publics forment les modèles linguistiques étendus (MLE) qui sous-tendent des outils tels que ChatGPT, mais pour les entreprises, les données privées et personnalisées constituent le principal facteur de différenciation. Les stratégies qui préservent la confidentialité et la souveraineté de ces données, tout en permettant à l'IA d'en tirer des leçons, sont essentielles pour obtenir un avantage concurrentiel.

C'est à cette intersection, entre les données d'entreprise et les systèmes intelligents, que le véritable potentiel de l'IA d'entreprise se concrétise. Ici, le contexte devient une capacité, et l'information devient une connaissance. Les entreprises capables d'exploiter cette relation de manière responsable définiront la prochaine ère de performance numérique.

L'IA peut-elle remplacer la gestion des données et des informations d'entreprise ?

Alors que l'adoption de l'IA augmente, la question qui revient souvent est de savoir si l'IA peut remplacer les solutions existantes de gestion des données et des informations. Pour faire court, la réponse est non. Toutefois, c'est l'intersection de la gestion de l'information et de l'IA qui est à l'origine des résultats. L'une ne peut pas agir sans l'autre. L'IA automatise les actions spécifiques aux données, telles que l'extraction et la classification des données, tandis que la gestion des informations fournit un contenu sécurisé et organisé et, surtout, une structure et des règles de base en matière de gouvernance et de conformité, ce que l'IA ne propose pas.

Alors que les solutions de gestion des données et des informations alimentent l'IA, l'IA transforme également la gestion de l'information. Elle la transforme via les aspects suivants :

- **Automatisation** - L'automatisation de l'IA étiquette les documents, génère des extraits, résume les rapports et réduit les erreurs humaines dans les principaux flux de travail.
- **Perspectives** - L'IA fournit des informations précieuses sur le contenu géré, notamment en obtenant des informations clés, des sentiments et d'autres notes importantes.
- **Recherche et extraction** - L'IA, associée aux métadonnées de la gestion de contenu, rend les interfaces de recherche plus précises, plus efficaces et plus faciles à utiliser.

La gestion de l'information est le garant de la fiabilité des données ; et la qualité des données détermine la crédibilité de chaque décision prise en matière d'IA. Les deux disciplines sont profondément liées : une IA efficace repose sur des données gouvernées et de haute intégrité, tandis que la gestion de l'information gagne en rapidité et en intelligence grâce à l'automatisation pilotée par l'IA. L'intégration de ces deux éléments garantit la cohérence, la conformité et le contexte tout au long du cycle de vie des informations (nous aborderons cela plus en détail au chapitre 5). L'IA peut améliorer la façon dont les entreprises gèrent le contenu, mais elle ne peut pas remplacer la discipline et la gouvernance qui garantissent la fiabilité des informations.

Cette interdépendance entre l'IA et la gestion de l'information est illustrée dans l'étude de cas suivante, qui présente un producteur alimentaire mondial appliquant l'IA à ses informations commerciales pour moderniser ses activités et améliorer ses performances.

Étude de cas

Un producteur mondial de produits alimentaires

Repérage des récoltes à l'aide de drones

Un fabricant de produits alimentaires présent dans le monde entier a mis en œuvre plusieurs stratégies pour se positionner en tant que leader du secteur en matière d'adoption de l'IA. Vous trouverez ci-dessous des extraits d'un entretien avec le directeur de la GIE de l'entreprise.

« Dans le cadre de notre projet de transformation, nous étudions comment l'intelligence artificielle peut nous aider à moderniser nos activités. Aujourd'hui, environ dix pour cent de nos données sont stockées dans le cloud. Ce n'est pas encore un gros chiffre, et les solutions cloud que nous avons utilisées jusqu'à présent sont restées privées afin de garantir la sécurité de nos informations propriétaires. Mais la technologie progresse rapidement et nous sommes de plus en plus ouverts à l'adoption du cloud public, à condition de garantir une gouvernance solide et de conserver la propriété de nos données.

L'IA joue un rôle central dans la façon dont nous gérons et tirons de la valeur de nos informations. Nous utilisons des systèmes basés sur l'IA pour tirer des informations de nos données opérationnelles, afin d'aider la direction à gérer nos usines de manière plus efficace. Les résultats sont tangibles : des produits de meilleure qualité, des pratiques plus durables et des améliorations mesurables du résultat net.

L'IA a également inspiré de toutes nouvelles méthodes de travail. Nous pilotons la surveillance des cultures par drone – le prolongement d'une pratique que nous utilisons depuis des années avec l'imagerie satellite. Les satellites nous ont aidés à évaluer la santé des cultures, mais ils ne sont pas très performants en cas de couverture nuageuse. Les drones, quant à eux, peuvent être programmés pour survoler des champs entiers, prendre des images en haute résolution et intégrer ces données directement à nos modèles d'IA. Une fois traités, les modèles prédisent les performances des cultures, identifient les tensions ou les maladies, et recommandent même des ajustements spécifiques en matière d'irrigation ou d'engrais. Ces mêmes informations sont ensuite intégrées dans des distributeurs d'engrais automatisés, qui appliquent la bonne quantité de traitement aux bons endroits, réduisant ainsi le gaspillage et améliorant le rendement.

Nous sommes également en train de passer à l'agriculture prédictive. En combinant des modèles d'IA avec des décennies de données météorologiques et agricoles historiques, nous pouvons prévoir les conditions de croissance dans deux à trois ans dans des régions spécifiques. Ces modèles ne sont pas parfaits, mais ils sont de plus en plus précis et incroyablement utiles pour la planification.

Chaque région du monde est différente : son sol, sa météo, ses cultures et ses agriculteurs. Notre défi est de nous adapter à chacun d'entre eux, et l'IA nous aide à le faire à grande échelle. La technologie nous permet de comprendre les conditions locales en temps réel et de prendre des décisions qui améliorent la productivité, la durabilité et la résilience. Ce qui nécessitait des semaines d'analyse manuelle se produit désormais en permanence. L'IA est devenue non seulement un outil d'information, mais aussi un partenaire dans la manière dont nous cultivons, produisons et nourrissons le monde. »

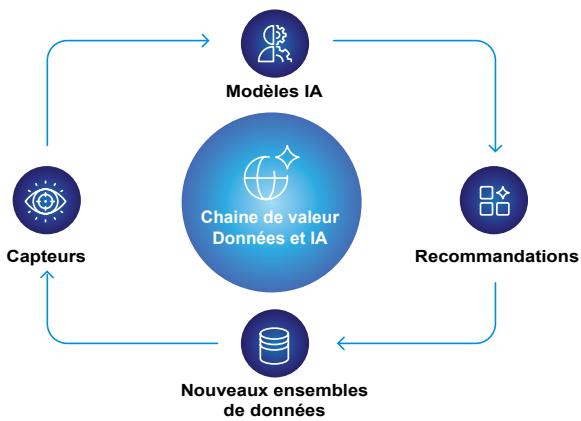
La chaîne de valeur des données et de l'IA

Pour tirer parti de la valeur des données, il faut d'abord comprendre les données et la chaîne de valeur de l'IA. Ce processus commence par la génération et la collecte de données, où l'accès aux données de l'entreprise devient un outil fondamental. Une fois collectées, les données doivent être intégrées, nettoyées et gérées pour garantir leur qualité et leur fiabilité. Les entreprises qui ont investi dans de solides pratiques de gestion de l'information sont mieux placées pour accélérer l'adoption de l'IA, car elles ont déjà effectué le travail fondamental d'activation de leurs données.

Cependant, les données à elles seules ne suffisent pas. Sans processus et flux de traitement structurés, les données ne sont pas exploitables. L'IA ne prend de la valeur que lorsqu'elle est appliquée à de véritables défis commerciaux, en s'intégrant à ces flux de traitement pour générer des résultats mesurables. C'est là qu'arrivent la formation, l'affinage et la validation des modèles d'IA. Les MLE sont initialement formés sur des ensembles de données publiques, mais les entreprises peuvent augmenter leur valeur en les affinant avec des données privées ou en utilisant des pipelines de génération améliorée par la recherche (GAR) qui connectent l'IA à des sources de connaissances internes. La bonne stratégie dépend des objectifs, des ressources et du niveau de maturité de l'entreprise. Cependant, quelle que soit l'approche, la qualité des données et la gouvernance des modèles sont des exigences essentielles.

La dernière étape, souvent négligée, de la chaîne de valeur est la boucle de rétroaction. De nombreuses entreprises s'empressent de déployer des capacités d'IA sans mettre en place de mécanismes d'apprentissage et d'amélioration continus. C'est là que la vraie valeur apparaît, en particulier avec l'IA. Le réglage itératif permet d'améliorer la précision du modèle au fil du temps et d'obtenir des résultats plus percutants.

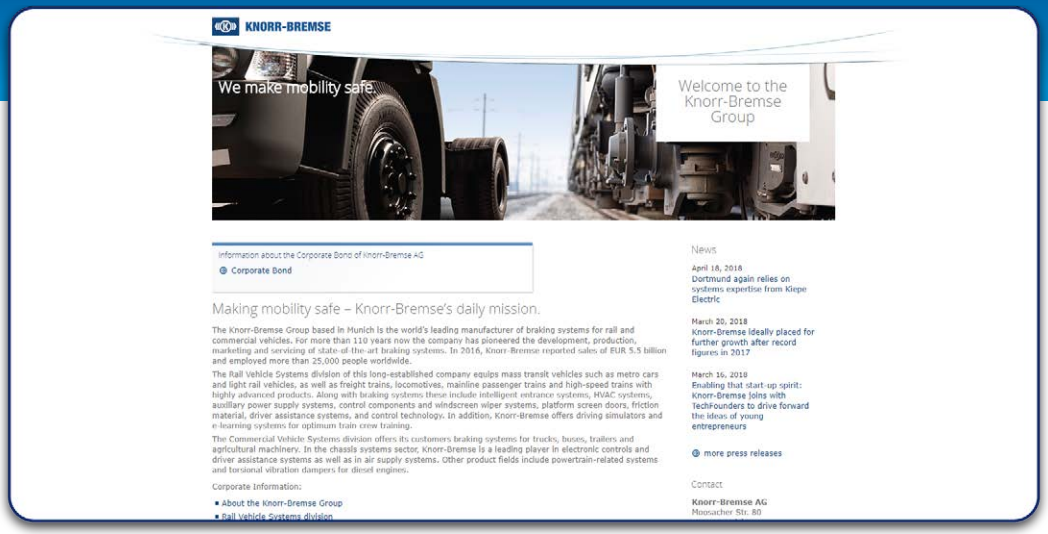
Pour replacer les données et la chaîne de valeur de l'IA dans leur contexte, prenons un exemple tiré du secteur manufacturier. Les capteurs de l'usine collectent des données, puis les introduisent dans les modèles d'IA. Sur la base de ces données, les modèles font des recommandations pour optimiser les performances. Cela génère à son tour de nouveaux ensembles de données qui peuvent être améliorés de manière continue et itérative.



Cette approche est démontrée dans l'étude de cas suivante, qui décrit comment Knorr-Bremse maintient le rythme grâce à une maintenance prédictive alimentée par des informations exploitables.

Étude de cas

Knorr-Bremse

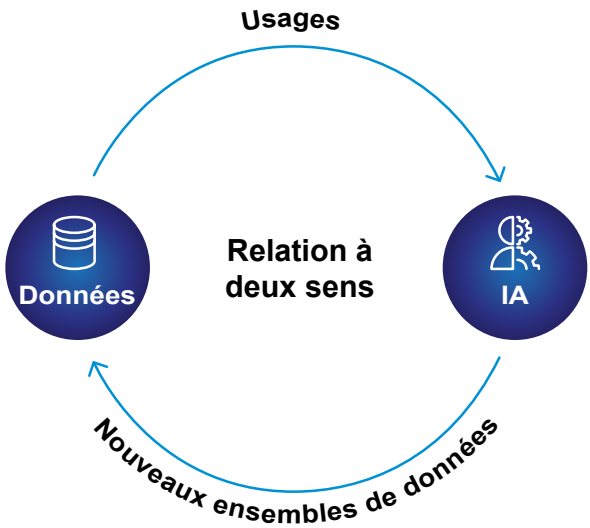


Groupe Knorr-Bremse

Basé à Munich, le groupe Knorr-Bremse est le premier fabricant mondial de systèmes de freinage pour véhicules ferroviaires et commerciaux. Depuis plus de 110 ans, l'entreprise est pionnière dans le développement, la production, la commercialisation et l'entretien de systèmes de freinage de pointe.

La plateforme iCom (intelligent Condition Oriented Maintenance – Maintenance orientée selon des conditions intelligentes) de Knorr-Bremse apporte la numérisation au secteur ferroviaire en connectant des capteurs sans fil à bord des trains à un réseau cloud de back-office, en utilisant un modèle IdO (Internet des objets). Cette plateforme transmet des données détaillées qui peuvent aider à prévoir les besoins de réparation et de remplacement. La plateforme iCom avait besoin d'un composant d'analyse puissant et convivial pour permettre l'analyse des données reçues afin d'aider les utilisateurs à prendre des décisions basées sur les données.

La capacité à prendre des décisions prédictives basées sur les données permet de réaliser des réparations plus efficaces et plus rentables. Les données étant collectées en permanence, les volumes d'une flotte sont considérables. Les clients ont désormais la possibilité de visualiser les données via des tableaux de bord graphiques interactifs, ce qui réduit la dépendance à l'égard de l'informatique pour créer de nouveaux rapports. Par exemple, ils peuvent fournir des cartes thermiques d'événements liés à l'état, tels que la surchauffe des freins sur une pente spécifique, aider les clients à mettre en place des mesures pour réduire les défaillances des composants, prolonger la durée de vie des pièces et, en fin de compte, économiser de l'argent.



L'IA et les données forment une relation bidirectionnelle

Les données, moteur de l'IA

Les données sont le carburant qui alimente le moteur d'IA. La quantité, la qualité et la diversité des données sont bien plus importantes que la complexité des modèles d'IA eux-mêmes. Des ensembles de données diversifiés et de haute qualité fournissent aux systèmes d'IA le contexte dont ils ont besoin pour apprendre efficacement. Une IA simple peut fournir des résultats impressionnants sur des ensembles de données variés et de haute qualité, tandis qu'une IA complexe ne peut pas fournir les mêmes résultats sur des ensembles de données homogènes et de faible qualité.

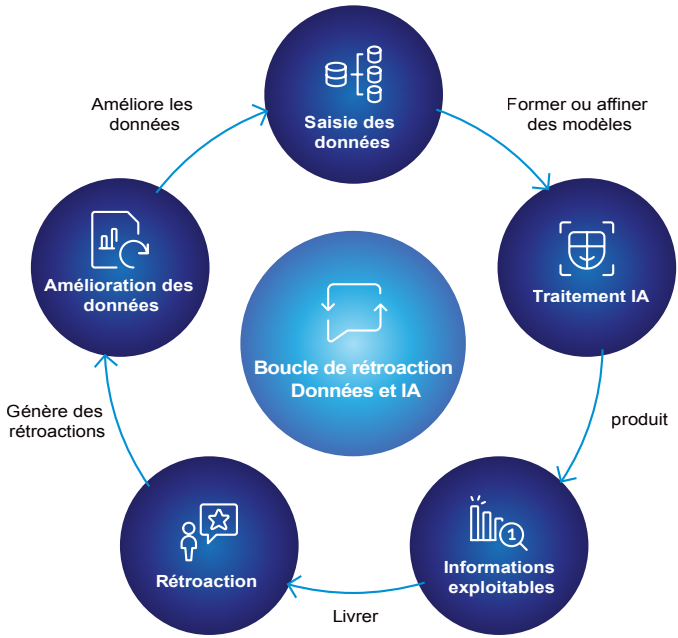
Comme nous l'expliquons dans le chapitre 1, les données structurées et non structurées alimentent cette combinaison. Débloquer ces données de manière sûre et responsable est la clé d'une adoption significative de l'IA dans les contextes commerciaux. Pour la plupart des entreprises, le succès ne dépend pas de la formation de grands modèles publics, mais de l'exploitation stratégique des données privées dans les cadres existants. Et une fois que ces données privées sont débloquées pour l'IA, il devient essentiel de les protéger. C'est la clé du concept de souveraineté dont nous parlerons plus loin dans le livre. Il est urgent de faire la différence entre les ensembles de données publics et privés et de fournir les protections appropriées aux ensembles de données privés.

L'IA ne se contente pas de consommer des données, elle les interprète, les enrichit et les organise pour les utiliser dans l'entreprise. En ce sens, l'IA et les données forment une relation bidirectionnelle. L'IA utilise les données pour apprendre, mais elle accroît également leur valeur en améliorant leur structure, leur intégrité et leur accessibilité.

La boucle de rétroaction continue

Tout système d'IA d'entreprise efficace utilise une boucle de rétroaction continue : les données forment les modèles d'IA, l'IA produit des informations, et ces informations génèrent de nouvelles données qui affinent à la fois le modèle et les ensembles de données sous-jacents. L'intelligence ne s'améliore pas en ligne droite, mais au fil des cycles d'apprentissage.

Par exemple, les systèmes de recommandation tirent constamment des leçons du comportement des utilisateurs. Chaque interaction génère de nouvelles données qui aident le système à établir de meilleures prévisions. Au fil du temps, ce raffinement itératif augmente la précision, la personnalisation et l'efficacité. Pensez à cela dans le contexte de votre site d'achats en ligne préféré. Chaque clic, achat ou pause crée de nouveaux signaux qui redéfinissent la compréhension par le système de l'intention de l'utilisateur. La prochaine série de recommandations reflète ce que le modèle a appris depuis la dernière. Il est formé pour vous fournir des recommandations pertinentes, mais au fur et à mesure que vous poursuivez vos achats, il utilise ces données pour générer de nouvelles informations et améliorer la qualité des recommandations au fil du temps.



L'IA et les données forment une relation bidirectionnelle

L'observabilité et le suivi sont tout aussi importants pour ce processus. La boucle doit être gouvernée et les modèles doivent évoluer de manière responsable. La surveillance continue des performances des modèles et du flux de données garantit que les systèmes d'IA restent fiables, explicables et conformes aux objectifs commerciaux. Comme nous le verrons plus loin dans le livre, la gestion opérationnelle des systèmes d'IA ne doit pas être une question secondaire ; elle doit être considérée comme une capacité stratégique qui sous-tend le succès à long terme.

La gouvernance à la croisée des chemins

La gouvernance est au cœur de l'intersection des données et de l'IA d'entreprise. Sur le plan des données, la gouvernance met l'accent sur la confidentialité, le lignage, le contrôle d'accès et le respect de réglementations telles que le RGPD (règlement général sur la protection des données). Du côté de l'IA, la gouvernance met l'accent sur l'équité, la transparence, la responsabilité et l'explicabilité.

Ces deux domaines se rejoignent désormais selon des principes communs tels que l'éthique, l'auditabilité et la confiance. Les nouveaux cadres de confiance en matière d'IA et les normes internationales, telles que la norme ISO/IEC 42001 pour la gestion de l'IA et la norme ISO/IEC 38505 pour la gouvernance des données, illustrent cette convergence. Au fur et à mesure que ces cadres arriveront à maturité, ils façonneront la manière dont les entreprises concevront, déploieront et surveilleront l'IA de manière responsable. Nous approfondirons la gouvernance des données et de l'IA dans les chapitres 5 et 6, respectivement.

> *L'intégration des données et de l'IA crée un avantage concurrentiel. C'est en les gérant de manière responsable que cela se transforme en valeur économique durablee.*

Implications stratégiques et économiques

Enfin, l'intégration des données et de l'IA crée à la fois un avantage stratégique et une opportunité économique. Les entreprises qui alignent efficacement ces capacités sont mieux équipées pour innover, optimiser leurs opérations et se différencier sur des marchés concurrentiels.

Avec autant d'anticipation de la part des conseils d'administration et des dirigeants sur le potentiel de l'IA d'entreprise, il est facile de comprendre une partie de la déception du marché concernant le rythme du changement et l'impact. Cela a mis en lumière les premiers projets pilotes d'IA en entreprise et leur succès relatif. Cependant, il convient de noter que de nombreux projets pilotes d'IA n'ont pas tenu leurs promesses parce qu'ils se sont appuyés sur des modèles formés par le public, sans avoir été contextualisés avec les données de l'entreprise. Les chefs d'entreprise doivent comprendre que leur avantage concurrentiel réside dans le fait de déverrouiller ces données en toute sécurité. La prochaine étape du succès consiste à adopter une approche de l'IA centrée sur les données qui priorise l'amélioration de la qualité des données et à la conception des processus, plutôt que de créer des modèles d'IA toujours plus complexes.

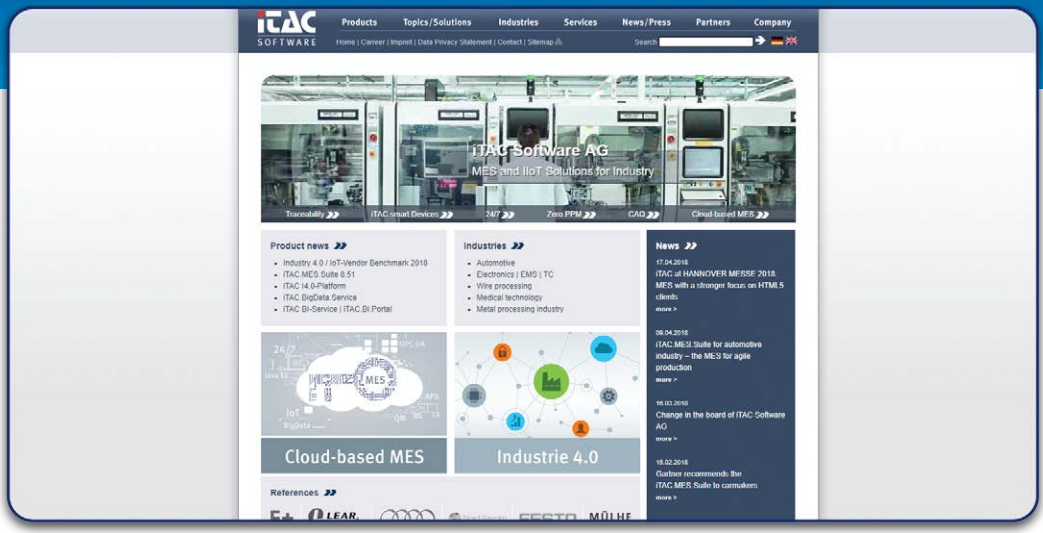
De bonnes données et de bons processus permettent d'obtenir des résultats fiables en matière d'IA.

Bien que l'informatique à grande échelle reste nécessaire à la formation des modèles de base, la plupart des entreprises peuvent obtenir une valeur significative grâce à des déploiements ciblés à plus petite échelle. Comprendre vos besoins en matière de données permet de déterminer le niveau d'investissement informatique réellement nécessaire, d'éviter les dépenses excessives et d'aligner les initiatives d'IA sur la valeur commerciale réelle. Cela contribue également à apaiser les inquiétudes des dirigeants et des employés qui cherchent peut-être encore à bien comprendre cette technologie.

Découvrez comment iTAC Software AG utilise l'intelligence pour créer des usines intelligentes dans cette étude de cas.

Étude de cas

iTAC Software AG



iTAC Software

Depuis sa création, iTAC (Internet Technologies and Consulting) Software AG se spécialise dans la fourniture de technologies Internet pour le secteur manufacturier. Ce fabricant de logiciels et de produits standard pour les applications informatiques interentreprises est un fournisseur de systèmes et de solutions de pointe pour les systèmes d'exécution de la fabrication (Manufacturing Execution Systems – MES) pour l'ensemble de la chaîne d'approvisionnement.

Pour offrir à ses clients la plus grande transparence possible et une capacité de prise de décision en matière de contrôle de production, et pour répondre à la demande croissante liée à l'Internet des objets (IdO), iTAC souhaitait intégrer des logiciels d'intelligence commerciale (IC) et d'analyse dans sa suite MES. Cela répondrait aux demandes des clients en matière d'intelligence de fabrication, de contrôle qualité et de traçabilité. Outre une mise en œuvre rapide et efficace et une intégration fluide, iTAC avait besoin de rapports personnalisés, d'analyses et de tableaux de bord avec une interactivité et une sécurité totales. Tout cela devait être basé sur le Web, proposer une personnalisation transparente pour les différentes applications et être disponibles via différents canaux.

iTAC dispose désormais des capacités IC, opérationnelles et analytiques dont elle a besoin pour répondre aux exigences de ses clients en matière d'intelligence, de contrôle de la qualité et de traçabilité tout au long du processus de fabrication. La solution garantit la transparence de la gestion des indicateurs et prend en charge la gestion du cycle de vie des produits, le contrôle du budget, l'assurance qualité, ainsi que la gestion des activités sur le terrain. Les clients de l'entreprise peuvent accéder à de grandes quantités de données et les analyser de manière centralisée grâce à un support extensible pour une expansion future, ce qui leur confère un avantage concurrentiel.

Comme nous l'avons indiqué dans ce chapitre, les données et l'IA sont des partenaires indissociables, les données étant le carburant du moteur de l'IA. L'IA sans données est sans direction, et les données sans IA ne sont pas exploitables. Ensemble, elles constituent la base d'une prise de décision intelligente en entreprise.

Alors que les entreprises s'orientent de plus en plus vers des cadres décisionnels basés sur l'IA, une gouvernance solide et un alignement stratégique deviennent essentiels. L'intersection des données et de l'IA représente non seulement un changement opérationnel, mais aussi une frontière en matière d'innovation, redéfinissant la façon dont les entreprises pensent, décident et se font concurrence. Cette convergence marque le début d'un nouveau chapitre de la transformation numérique, dans lequel les informations deviennent véritablement des informations.

Télécharger The Fast Five

1. **Donnez la priorité à la qualité et à la gouvernance des données.**
   Établissez la préparation des données comme un mandat organisationnel, et non comme un élément livrable du projet. Demandez à vos équipes de réaliser des audits complets des données et de mettre en œuvre des politiques de gouvernance garantissant l'exactitude, la sécurité et l'accessibilité de tous les actifs d'information essentiels. Faites de la qualité des données une priorité du conseil d'administration afin de maximiser l'efficacité de l'IA.

2. **Intégrez l'IA à de véritables flux de traitement commerciaux.**
   Intégrez l'IA aux processus commerciaux à fort impact afin d'identifier deux à trois domaines opérationnels clés (par exemple, le support client, l'optimisation de la chaîne d'approvisionnement, la gestion des risques) dans lesquels elle peut apporter des avantages immédiats. Chargez les responsables commerciaux et techniques de déployer des solutions d'IA qui exploitent des données propriétaires pour relever de véritables défis commerciaux.

3. **Établissez des boucles de rétroaction continues pour améliorer l'IA.**
   Les performances de l'IA ne sont jamais statiques ; elles nécessitent une surveillance et une formation continues. Instituez une politique d'entreprise pour le suivi continu des performances des modèles d'IA, y compris les boucles de rétroaction des utilisateurs et le recyclage automatique à l'aide de nouvelles données. Attribuez la responsabilité de ce processus afin de garantir que les modèles restent précis, personnalisés et conformes aux objectifs commerciaux.

4. **Alignez la gouvernance des données et de l'IA pour garantir la confiance et la conformité.**
   Réunissez les données et l'IA dans un cadre de gouvernance unique. Désignez un groupe de travail interfonctionnel qui associe confidentialité, sécurité, conformité et supervision éthique afin de créer des normes cohérentes sur la manière dont le renseignement est créé et appliqué. Adoptez des normes émergentes (telles que ISO/IEC 42001 et 38505) ou vous y référer pour gérer de manière proactive les risques juridiques, opérationnels et de réputation.

5. **Adoptez une approche centrée sur les données pour investir dans l'IA.**
   Liez toutes les décisions d'investissement à la valeur des données et aux résultats commerciaux. Avant d'approuver de nouveaux projets d'IA, demandez aux unités commerciales d'expliquer comment l'initiative permet de tirer parti des données de l'entreprise et d'obtenir des résultats commerciaux mesurables. Limitez les investissements dans des modèles d'IA à grande échelle, sauf si cela est justifié par des actifs de données uniques et une trajectoire claire vers le retour sur investissement.

Chapitre quatre

La sécurisation : l'importance de la cybersécurité

L'innovation doit être équilibrée par la confiance, afin de garantir que l'intelligence que nous construisons ne puisse pas être utilisée contre nous. Dans ce chapitre, nous explorons comment la cybersécurité doit évoluer parallèlement à l'IA. Alors que les systèmes intelligents redéfinissent le mode de fonctionnement des entreprises, les nouveaux risques exigent des défenses tout aussi avancées. Nous examinerons les menaces émergentes, ainsi que les stratégies nécessaires pour sécuriser les données, les modèles et les opérations de lutte pilotées par l'IA contre ces menaces.

> *62 % des entreprises ont été victimes d'une attaque deepfake impliquant de l'ingénierie sociale ou exploitant des processus automatisés, tandis que 32 % ont déclaré avoir été victimes d'une attaque contre des applications d'intelligence artificielle exploitant le processus de prompt au cours des 12 derniers mois.* [23]

Ces dernières années, les cybermenaces sont passées de simples infractions à des attaques sophistiquées visant directement les systèmes d'IA des entreprises, et les enjeux n'ont jamais été aussi élevés. Alors que les entreprises accélèrent l'adoption de technologies telles que l'IA générative (GenAI), nous assistons à une recrudescence des attaques qui exploitent l'IA à des fins de phishing (hameçonnage)4, de deepfakes et d'ingénierie sociale avancée. Dans le même temps, une nouvelle vague de vulnérabilités fait son apparition : des acteurs malveillants exploitent l'infrastructure GenAI, manipulent des instructions ou compromettent des chaînes de flux de traitement d'IA pour infiltrer et perturber les entreprises.

Dans le chapitre précédent, nous avons examiné comment l'intersection des données et de l'IA d'entreprise crée des opportunités d'innovation et d'efficacité opérationnelle. Mais les opportunités s'accompagnent également de risques indésirables, et à mesure que les organisations s'appuient sur des données privées pour alimenter leurs moteurs d'IA, elles peuvent s'exposer par inadvertance à de nouveaux cyber-risques en constante évolution. La protection des données d'entreprise et de l'IA doit suivre le rythme de l'évolution technologique, car les données et l'IA sont des cibles attrayantes pour les cybercriminels.

Dans l'article suivant, une entreprise du secteur de l'énergie jette les bases de l'IA et de l'analyse avancée au sein d'un système GIE sécurisé, en élaborant une architecture d'entreprise qui associe ses données aux processus de gouvernance et de contrôle de cybersécurité.

Étude de cas

Une société énergétique du Nord

Cette entreprise de production d'énergie opère dans un secteur hautement réglementé et gère d'importants volumes de documentation technique essentielle à la sécurité et aux activités. Confrontée au défi de permettre à plus de 900 employés d'accéder de manière fiable aux dernières versions approuvées de ses documents dans des environnements de bureau et d'usine, l'entreprise a reconnu que les anciens systèmes fragmentés n'offraient pas la gouvernance et la visibilité requises pour une gestion moderne des risques et de la confiance. À une époque où les données sont à la fois un atout et une vulnérabilité, il est devenu impératif d'adopter une approche axée sur la sécurité dès la conception.

Pour établir une base solide, l'entreprise a mis en place un environnement de gestion de contenu unifié fondé sur de solides contrôles d'identité et d'accès, une automatisation des flux de traitement et une gouvernance du cycle de vie des documents. En centralisant le contrôle et en appliquant des droits d'accès définis par des politiques, le système a veillé à ce que seuls les utilisateurs appropriés puissent accéder aux dossiers opérationnels sensibles, au bon moment et dans le bon contexte. Les flux de traitement automatisés ont fait passer les documents à la révision, à l'approbation et à l'archivage de manière contrôlée, renforçant ainsi la sécurité du plan de données tout en préservant la convivialité pour les équipes de terrain comme pour les équipes de bureau. Avec cette architecture en place, l'organisation a jeté les bases d'analyses avancées et de fonctionnalités basées sur l'IA, étant entendu que celles-ci doivent reposer sur des informations sécurisées et bien gérées.

Les résultats ont été marquants. L'entreprise a obtenu un excellent bilan de stabilité et a considérablement amélioré la productivité des utilisateurs, grâce à un accès en temps quasi réel à des contenus critiques garantissant à la fois la sécurité et l'intégrité opérationnelle. Mais ce qui est peut-être plus important encore : ils possèdent désormais l'infrastructure d'information fiable nécessaire pour introduire des outils de recherche, de recommandations et d'aide à la décision pilotés par l'IA, de manière sécurisée et responsable. Bref, en considérant la cybersécurité, la gouvernance des données et la préparation à l'IA comme des éléments étroitement liés, l'entreprise est passée de la gestion de documents à une plateforme intelligente moderne, ancrée dans la confiance, la visibilité et l'automatisation.

> *Nous passons plus de 70 % de notre temps à nous défendre contre la technologie, autant contre des réglementations que de menaces de cybersécurité. Nous devons rester vigilants pour protéger la banque et les données de nos clients et suivre les derniers changements et correctifs qui corrigent les vulnérabilités.*
>
> Directrice technique et directrice générale d'une banque mondiale

Le paysage des cybermenaces pour les données et l'IA

Selon les *Perspectives mondiales de cybersécurité 2025* du Forum économique mondial, « les outils GenAI redéfinissent le paysage de la cybercriminalité en permettant aux criminels d'affiner leurs méthodes, d'automatiser et de personnaliser leurs techniques. 47 % des entreprises ont indiqué que leur principale préoccupation concernant l'IA est le développement des capacités antagonistes. Les cybercriminels exploitent l'efficacité de l'IA pour automatiser et personnaliser des communications trompeuses. Environ 42 % des entreprises ont été victimes d'une attaque d'ingénierie sociale réussie au cours de l'année écoulée, un chiffre qui ne peut qu'augmenter avec les avancées et l'adoption malveillante de l'IA. » [24]

La cybersécurité pour l'IA d'entreprise doit être abordée d'un point de vue multidimensionnel –une perspective qui englobe le spectre complet des menaces couvrant les données, les modèles, l'infrastructure et l'interaction humaine. Le paysage des cybermenaces pour les données et l'IA touche à l'infrastructure, à la gouvernance et au comportement humain. Les cyberrisques traditionnels, tels que les accès non autorisés, les menaces internes et les ransomwares (rançongiciels), continuent de cibler les systèmes des entreprises et de compromettre des données critiques. Et comme les entreprises transfèrent toujours plus de données et d'opérations dans des environnements cloud, la surface d'attaque globale continue de croître. Les cybercriminels continuent d'exploiter les faiblesses de la gestion des identités, de la segmentation du réseau et des logiciels vulnérables. Ces menaces fondamentales créent les conditions nécessaires à des formes d'attaque plus avancées qui exploitent la dépendance croissante à l'égard de l'IA.

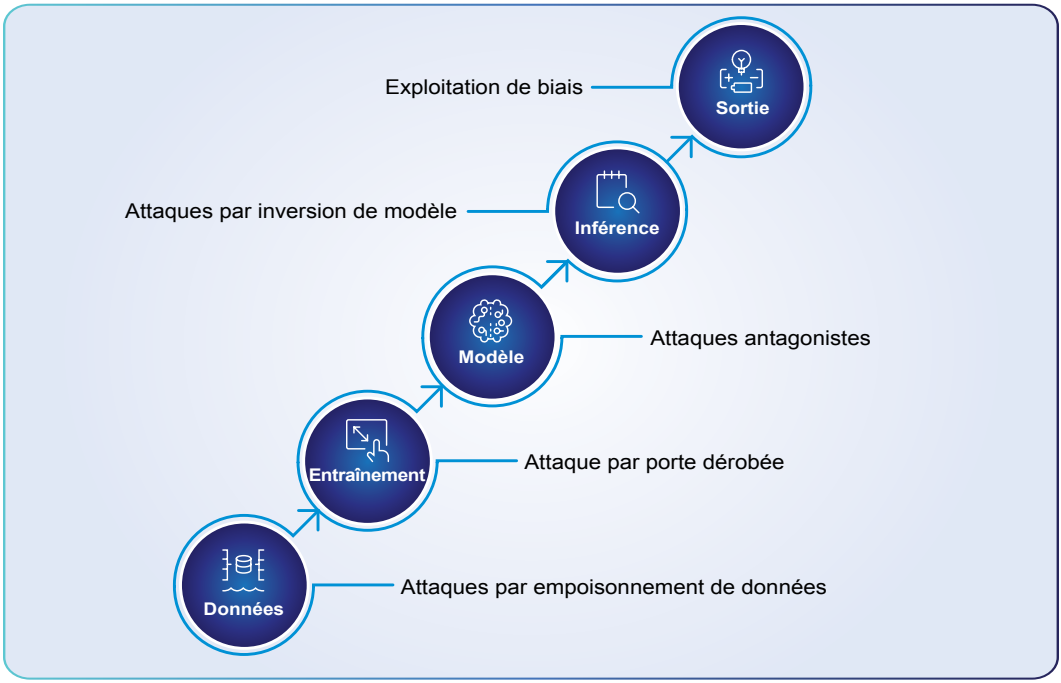
Parmi les surfaces d'attaque en expansion, citons les pipelines de données utilisés pour entraîner les MLE et les modèles eux-mêmes. Comme l'ont observé des chercheurs d'IBM et de l'université Carnegie Melon : « Le nombre croissant d'applications utilisant des modèles linguistiques étendus (MLE) conçus par un tiers soulève de graves inquiétudes quant à la vulnérabilité des MLE en matière de sécurité. Il a été démontré que des acteurs malveillants peuvent exploiter secrètement ces vulnérabilités des MLE par le biais d'attaques par empoisonnement visant à générer des résultats indésirables. » [25]

Outre l'empoisonnement des modèles, d'autres risques de sécurité, tels que l'exfiltration de données et l'injection rapide, sont de plus en plus courants, ce dernier point constituant l'un des principaux défis de sécurité en matière de MLE.

Les nouvelles menaces spécifiques à l'IA introduisent de nouvelles vulnérabilités qui vont au-delà des vols de données classiques. Comme de nouvelles menaces apparaissent chaque jour, il est impossible de dresser une liste complète et à jour des attaques. Cependant, parmi les types les plus courants, citons :

- Attaques par empoisonnement de données
- Attaques par porte dérobée
- Attaques antagonistes (évasion)
- Attaques par inversion du modèle
- Attaques pa exploitation de biais

Le schéma ci-dessous montre le cycle de vie du modèle d'IA en fonction des différents types de cyberattaques que nous allons examiner dans cette section. Le cycle de vie commence par la collecte et la préparation des **données**, puis par la phase d'**entraînement** au cours de laquelle le **modèle** apprend. Il en résulte un modèle entraîné, qui est ensuite utilisé pour l'**inférence** (le processus de prévision ou de décision) afin de générer le **résultat** final (une prédiction, une classification, une décision ou une réponse générée).



Cartographie des cyberattaques sur des modèles d'IA

Comprendre le lien entre ces différentes cyberattaques et le cycle de vie des modèles d'IA permet de les situer dans le contexte dans lequel les menaces peuvent survenir. Examinons les menaces plus en détail.

1. Empoisonnement des données

Les attaques par empoisonnement des données sont fréquentes pendant la phase de collecte des données qui précède l'entraînement, lors de la collecte et de l'ingestion. Dans le cadre de ces attaques, les acteurs malveillants injectent des informations malveillantes dans le jeu de données d'entraînement, corrompant ainsi la façon dont le modèle apprend, ce qui compromet son intégrité et sa fiabilité. Le problème réside dans une hypothèse erronée : la plupart des algorithmes d'apprentissage partent du principe que les données d'entraînement sont propres et représentatives de la réalité. Dans les environnements sensibles sur le plan de la sécurité, cette hypothèse est tout simplement fausse. [26]

2. Attaques par porte dérobée

Les attaques par porte dérobée sont une forme d'empoisonnement des données qui consiste à masquer un schéma déclencheur dans le modèle pendant l'entraînement. Le modèle se comportera normalement pour les entrées normales, mais produira ensuite un résultat malveillant lorsque le déclencheur apparaît. Ces types d'attaques peuvent être compliqués à détecter car ils restent inactifs jusqu'à ce que la condition de déclenchement soit remplie. Dans ce cas, « un adversaire peut créer un réseau entraîné de manière malveillante (un réseau neuronal BadNet) qui présente des performances de pointe sur les échantillons d'entraînement et de validation de l'utilisateur, mais qui se comporte mal sur des données d'entrée spécifiques choisies par l'attaquant ». [27]

3. Attaques antagonistes

Un autre type d'attaque courant est l'attaque antagoniste. Celles-ci se produisent lorsque les acteurs malveillants tentent de manipuler les entrées du modèle IA pour produire des résultats incorrects. Ces changements sont parfois si minimes qu'ils ne sont pas reconnaissables, mais ils peuvent modifier le comportement et compromettre la sécurité dans des cas d'utilisation de l'IA tels que l'imagerie médicale ou la navigation autonome. [28]

4. Attaques par inversion de modèles

Les attaques par inversion de modèle constituent une menace pour la vie privée et les données personnelles. À cette fin, elles tentent de « reconstruire les données d'entrée sensibles à partir des paramètres, des résultats ou des représentations intermédiaires du modèle ». [29] En d'autres termes, l'attaque consiste essentiellement en une rétro-ingénierie du modèle afin d'exposer les données spécifiques et privées à partir desquelles il a été formé.

5. Attaques par exploitation de biais

Le dernier type d'attaque que nous allons mettre en évidence est celui des attaques par exploitation de biais, qui tirent parti des distortions (biais) déjà présents dans l'ensemble de données pour manipuler la prise de décision. Ces attaques sont différentes d'un empoisonnement des données, car elles n'introduisent pas de nouvelles données dans l'ensemble de données. Au lieu de cela, elles exploitent les inégalités inhérentes déjà présentes dans les données pour mener à bien une attaque. [30]

Dans les secteurs public et privé, les risques vont désormais au-delà des compromissions techniques (comme l'accès au système) pour inclure la manipulation des données (comme la modification ou l'empoisonnement des données). Il ne s'agit que de cinq exemples, montrant comment les cyber-criminels s'attaquent à différentes parties du cycle de vie du modèle IA. Par exemple, dans le secteur public, les gouvernements ont été confrontés à des attaques de rançongiciels contre des infrastructures publiques qui ont eu un impact sur des services essentiels. De même, dans le secteur privé, les entreprises ont été victimes d'interférences de modèles de la part de cyber-criminels qui ont une incidence sur leurs sites Web et leurs systèmes de recommandation.

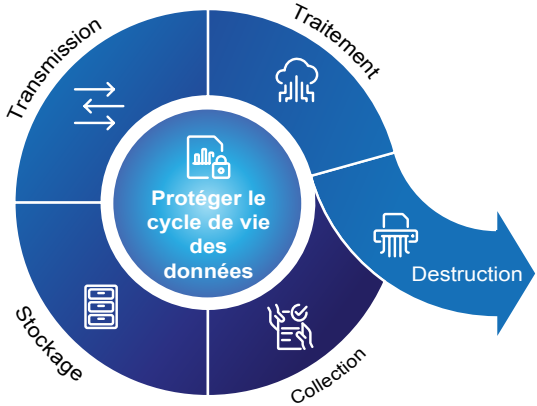
Plus généralement, la GenAI a été utilisée pour diffuser de la désinformation. Ces attaques tirent parti de la partialité des modèles et érodent la confiance du public dans l'IA. Ces cas montrent que la cybersécurité des données d'entreprise et de l'IA ne se limite plus à la protection des systèmes. Il s'agit de défendre l'intégrité des données et des décisions et de conserver la confiance du public dans l'ère cognitive.

Les bases de la sécurité des données

Cet examen des menaces met en lumière un thème central : les données utilisées pour former les modèles d'IA des entreprises doivent être sécurisées. À mesure que les entreprises intensifieront leur utilisation de l'IA, le volume et la sensibilité des données qu'elles gèrent continueront de croître de façon exponentielle. Souvenez-vous du nombre de paramètres utilisés pour entraîner de petits et grands modèles linguistiques et de la façon dont le volume augmente à mesure que nous arrivons à l'IAG. Pour les entreprises qui exploitent des ensembles de données privés pour créer une IA privée, il est essentiel de garantir la confidentialité et l'intégrité de ces données tout au long de leur cycle de vie. Pour établir cette base, il faut adopter une approche de « sécurité dès la conception », combinant de solides contrôles techniques à de robustes mécanismes de gouvernance. Cette stratégie est essentielle pour protéger les informations tout en respectant les normes et réglementations.

Protéger le cycle de vie des données

En général, les données passent par différentes phases pendant leur cycle de vie, notamment la collecte, le stockage, la transmission (distribution), le traitement (archivage et conservation) et la destruction. La protection des données à chaque étape nécessite une combinaison de contrôles préventifs, de détection et correctifs pour se défendre contre les cybermenaces.



Cartographie des cyberattaques sur des modèles d'IA

Collecte

La collecte de données doit être effectuée avec soin, car elle peut compromettre les données. Il est essentiel de comprendre quelles données sont collectées et à quelles fins. La norme ISO/IEC 27001:2022 fournit un cadre qui aide les entreprises à comprendre comment protéger les informations tout au long de leur cycle de vie. Elle propose un ensemble de catégories de contrôle pour garantir que la collecte et le traitement des données soient licites, équitables et transparents. [31]

Stockage

Une fois que les données ont été collectées sans risque, elles doivent être stockées en toute sécurité. Cela peut être dans une infrastructure sur site ou dans un environnement cloud. La protection générale des données inclut le chiffrement au repos, les contrôles d'accès et la séparation des données sensibles. Cela peut également inclure des fonctionnalités telles que le stockage immuable, qui peut s'inscrire dans le cadre d'une stratégie plus large de protection des données visant à atténuer les cyberattaques telles que les rançongiciels. Cela doit faire partie de la stratégie de protection des données Zero Trust de votre entreprise (nous y reviendrons prochainement).

Transmission

Les données transmises ou distribuées entre les systèmes sont vulnérables aux interceptions. Pour protéger ces données en transit, des méthodologies techniques telles que le cryptage sont utilisées. Le cryptage n'empêche pas l'interception des données, mais il les rend inutilisables si elles le sont. [32]

Traitement

La phase de traitement des données est un point critique au cours duquel les données peuvent être interceptées ou manipulées. Des contrôles d'accès stricts sont donc essentiels pour empêcher tout accès non autorisé. À ce stade, le principal risque concerne les atteintes à la vie privée, en particulier lorsque des ensembles de données sensibles sont utilisés pour la formation ou l'analyse de modèles d'IA. Pour atténuer ces risques, de nouvelles méthodes de calcul ont été développées. Le chiffrement homomorphe, par exemple, préserve la confidentialité en permettant d'effectuer des opérations sur des données cryptées sans les déchiffrer. En outre, l'apprentissage fédéré représente une évolution vers une IA distribuée et sécurisée. Cela permet aux modèles d'être entraînés localement sur plusieurs ensembles de données décentralisés. Cette approche, « Apporter le code aux données », minimise le besoin de centraliser les données sensibles, réduisant ainsi les risques d'exposition tout en préservant les performances du modèle. [33]

Élimination ou suppression de données

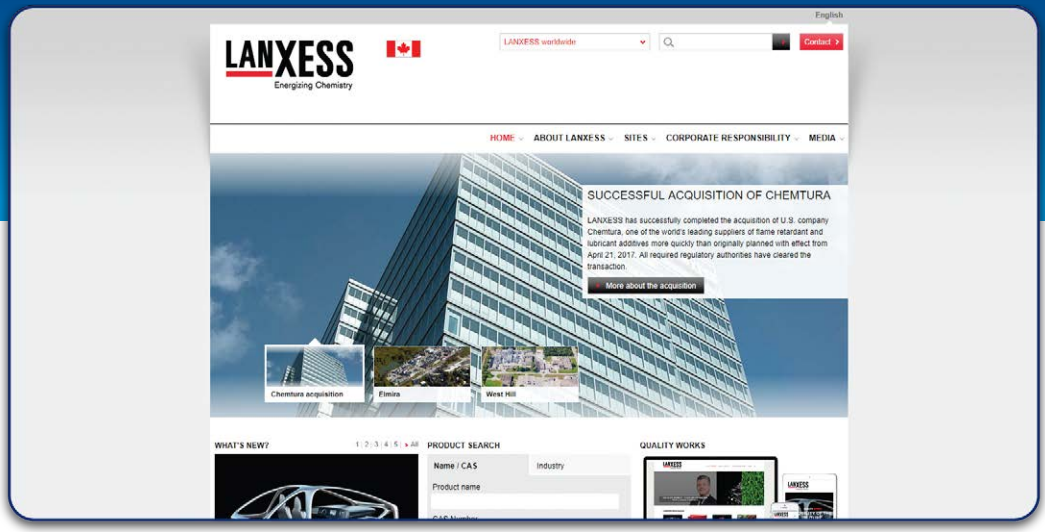
La suppression sécurisée des données est la dernière étape et garantit la suppression définitive des données anciennes ou redondantes. En vertu des réglementations relatives à la protection de la vie privée, telles que l'article 17 du RGPD, il existe un « droit à l'effacement » ou un « droit à l'oubli », ce qui signifie que les entreprises doivent démontrer qu'elles ont correctement exécuté les demandes de suppression. [34]

Chaque étape du cycle de vie des données est interdépendante, et une faiblesse de l'une d'entre elles peut compromettre l'ensemble du cycle de vie. Comprendre les risques tout au long du cycle de vie garantit que vous avez pris en compte tous les aspects lors de l'élaboration d'une stratégie de protection des données Zero Trust.

Dans l'étude de cas suivante, une entreprise du secteur chimique de premier plan utilise un système de gestion des informations d'entreprise pour gérer le cycle de vie de ses données, assurer la conformité et sécuriser ses données sur de multiples processus, partenaires et sites.

Étude de cas

LANXESS



LANXESS

Le cœur de métier de LANXESS est le développement, la fabrication et la commercialisation d'intermédiaires chimiques, d'additifs, de produits chimiques spécialisés et de plastiques. Vous trouverez ci-dessous des extraits d'un entretien avec un expert en processus GCE de l'entreprise.

« Compte tenu de la complexité de notre portefeuille, lorsque nous fabriquons des produits (intermédiaires chimiques, additifs, produits chimiques spécialisés et plastiques), nos processus laissent des traces écrites issues de la recherche scientifique, des ventes et du marketing.

Le point de départ habituel d'une recherche est lorsqu'un client demande une nouvelle fonctionnalité du produit. En général, nous menions des recherches avec un partenaire externe. Il y avait donc des exigences en matière d'accès sécurisé et de collaboration. Parce que nous sommes une entreprise qui fabrique et distribue dans le monde entier, nos produits, nos activités et nos traces écrites doivent être conformes aux réglementations internationales.

Une plateforme de gestion de contenu d'entreprise (GCE) nous aide à garantir la conformité des informations, qu'il s'agisse des recherches menées, des procédures établies par les ingénieurs pour fabriquer à grande échelle, de la construction et de l'exploitation d'une usine, et enfin, des ventes et du marketing. Nous traitons de gros volumes de papier tous les jours. Chaque étape d'un processus doit être conforme et bien documentée, d'autant plus que nous opérons dans 25 pays et que chacun est soumis à un ensemble de réglementations différent.

La conformité est un avantage résultant d'une gestion efficace de l'information, au même titre que l'efficacité et la productivité – en particulier la possibilité de trouver l'information plus rapidement. Pour bénéficier de ces avantages, nous devons montrer à nos clients internes en quoi l'utilisation de cette technologie leur facilitera la tâche. La GCE fournit les outils dont nous avons besoin pour trouver un équilibre entre conformité, sécurité et facilité d'utilisation. »

Architecture Zero-Trust pour l'IA d'entreprise

Nous avons passé en revue les cybermenaces liées aux données et à l'IA, en nous concentrant spécifiquement sur le cycle de vie des données et les points où les attaques peuvent se produire. Pour se protéger contre ces menaces, le National Institute of Standards and Technology (NIST) définit une architecture Zero-Trust comme une approche stratégique de la cybersécurité qui suppose l'absence de confiance implicite au sein d'un réseau. Le modèle est basé sur l'idée qu'il ne faut jamais faire confiance et qu'il faut toujours vérifier, et cette philosophie doit régir chaque décision d'accès. Au lieu de s'appuyer sur des moyens de défense tels que des pare-feu ou des VPN, Zero-Trust utilise la vérification continue et le contrôle d'accès pour tous les actifs, utilisateurs et flux de données.

Selon le NIST SP 800-207, le modèle Zero-Trust redéfinit la sécurité d'entreprise traditionnelle en se concentrant sur :

- **Protection centrée sur l'identité** : Chaque demande d'accès doit être authentifiée et autorisée en temps réel.
- **Accès au moindre privilège** : les utilisateurs et les systèmes ne bénéficient que du niveau d'accès minimum nécessaire pour exécuter leurs opérations.
- **Application dynamique des politiques** : les décisions d'accès sont évaluées en temps réel en fonction de facteurs tels que le comportement des utilisateurs et la sensibilité des données.
- **Microsegmentation** : Les réseaux sont divisés en petites zones isolées afin de limiter les déplacements des cybercriminels en cas de compromission.
- **Visibilité et analyse** : La surveillance et la détection des menaces continues garantissent que certains comportements déclenchent des réponses automatisées.

Le modèle Zero-Trust n'est pas une solution unique. Il est réalisé grâce à une combinaison de solutions technologiques, notamment la gestion des identités et des accès (GIA), l'authentification multifactorielle (AMF), le chiffrement, la surveillance continue et l'application automatisée des politiques. [35] L'IA GIA deviendra un composant de sécurité essentiel de tout système d'entreprise.

Découvrez comment une société de divertissement latino-américaine s'efforce de combiner ces solutions technologiques dans le cadre de son plan visant à passer à un modèle de sécurité Zero-Trust dans l'article ci-dessous.

Étude de cas

Une société de divertissement latino-américaine

Avec des millions de clients et des milliers d'employés dans de nombreux pays, une grande entreprise de divertissement latino-américaine a dû faire face à des défis croissants en matière de gestion de l'identité et des accès pour un effectif nombreux et dispersé. Au fil du temps, la fragmentation des systèmes et le provisionnement manuel ont rendu difficile le maintien de la visibilité sur 15 000 identités d'utilisateurs et plus de 400 applications. L'absence de gouvernance unifiée a ralenti les temps de réponse, créé des angles morts en matière de sécurité et rendu plus difficile la transition vers un modèle Zero-Trust.

Pour y remédier, l'entreprise a mis en œuvre un cadre complet de gouvernance et d'administration des identités (GIA), consolidant les données d'identité mondiales en une source unique de vérité et un point de contrôle central. Intégrée aux systèmes RH, à Active Directory et à des dizaines d'applications d'entreprise, la plateforme a automatisé le provisionnement, le déprovisionnement et la révision des accès, réduisant ainsi de moitié la charge de travail manuelle. Les alertes intelligentes, les attestations continues et les contrôles d'accès basés sur les rôles ont renforcé la conformité, minimisé les risques et imposé le principe du moindre privilège au sein de l'entreprise.

Les résultats ont été immédiats. L'entreprise a acquis une visibilité de bout en bout sur plus de 15 000 identités, a rationalisé la gestion des accès et a renforcé sa sécurité sur le marché mondial. La gouvernance des identités étant désormais au cœur de sa stratégie de cybersécurité, l'entreprise est bien placée pour développer son modèle Zero Trust, en appliquant la même rigueur et la même automatisation à la protection de ses données, de ses applications et de ses opérations basées sur l'IA dans l'ensemble de l'entreprise numérique.

Sécurité de l'IA et protection des modèles

Le modèle Zero-Trust, comme nous venons de le voir, définit une philosophie et une stratégie pour protéger l'accès, mais nous devons également prendre en compte la sécurité de l'IA et la protection des modèles de manière plus générale. Les modèles d'IA diffèrent des systèmes informatiques traditionnels dans la mesure où ils associent logique et capacité à tirer des leçons des données en continu. Nous avons examiné plus tôt les surfaces d'attaque tout au long du cycle de vie des modèles d'IA.

Pour se protéger contre ces risques, les entreprises adoptent des stratégies qui combinent des approches classiques en matière de cybersécurité avec de nouvelles approches. Il peut s'agir de former les équipes et les modèles aux approches d'attaques adverses, aux modèles de filigrane, et de passer des tests effectués par une équipe rouge à leurs environnements de pré-déploiement. Dans ce contexte, une équipe rouge est un groupe qui simule des cyberattaques réelles pour tester la sécurité d'une entreprise. Leur objectif est de détecter les faiblesses des systèmes, des réseaux et des personnes.

L'entraînement peut améliorer les performances des modèles en les exposant à des exemples contradictoires pendant l'entraînement, augmentant ainsi leur résilience face aux attaques contradictoires. [36] Le filigrane des modèles fournit une assurance et aide à identifier la réutilisation non autorisée des modèles. [37] Les tests de l'équipe rouge sont utiles pour exposer les vulnérabilités par le biais d'attaques simulées avant le déploiement.

En combinaison avec une approche Zero-Trust, il peut s'agir de tactiques puissantes pour se protéger contre les attaques. Toutefois, il ne s'agit que de quelques approches potentielles parmi d'autres, qui doivent être définies dans le cadre d'une stratégie globale d'IA à l'échelle de l'entreprise.

Perspectives d'avenir : l'avenir de la cybersécurité pour l'IA

Ce chapitre a examiné l'importance croissante de la cybersécurité par rapport à l'IA d'entreprise, en mettant en lumière le nombre croissant de cyberattaques visant les systèmes d'IA des entreprises. Alors que des rapports indiquent que 62 % des entreprises ont été victimes de fausses attaques et que l'on s'inquiète de la capacité contradictoire des IA générales, il est évident qu'il est urgent de faire face aux cyber-risques liés à l'IA et aux données. Pendant que les entreprises exploitent les données privées pour améliorer leur efficacité opérationnelle, elles s'exposent simultanément à des vulnérabilités complexes qui menacent leurs modèles et leurs données d'IA.

Nous avons également analysé le fonctionnement de ces attaques, en mettant en évidence les menaces telles que l'empoisonnement des données, les attaques par porte dérobée et les attaques par inversion. Ces risques mettent en lumière certaines des limites des approches traditionnelles de cybersécurité en matière de protection des systèmes d'IA avancés. En comprenant le lien entre ces attaques et les différentes phases du cycle de vie des modèles d'IA, les entreprises peuvent mieux anticiper les vulnérabilités potentielles et mettre en œuvre des stratégies de protection des données et de sécurité des modèles.

Pour l'avenir, les entreprises doivent adopter des cadres de cybersécurité proactifs et adaptatifs qui intègrent des approches de défense axées sur l'IA pour contrer les attaques effectuées par l'IA. Cela inclut le développement de systèmes intelligents de détection des menaces et de nouveaux modèles d'évaluation des risques. En fin de compte, la collaboration entre les secteurs public et privé, associée à l'investissement dans des solutions de cybersécurité innovantes, sera essentielle pour devancer l'évolution du paysage des menaces et garantir l'intégration sûre des technologies IA dans les opérations de l'entreprise.

Au fur et à mesure que les entreprises renforcent leurs cyberdéfenses, une vérité s'impose : sécurité et confiance sont indissociables. Protéger les systèmes IA des entreprises ne consiste pas seulement à se défendre contre les attaques, il s'agit également de garantir que les données qui alimentent ces systèmes restent exactes, éthiques et fiables. Dans le chapitre suivant, nous explorerons le fondement d'une IA fiable : la gouvernance des données.

Télécharger The Fast Five

1. **Adopter une architecture Zero-Trust pour tous les systèmes de données et d'IA.** Mettez immédiatement en œuvre un modèle de sécurité Zero Trust qui suppose l'absence de confiance implicite au sein de votre réseau. Appliquez des politiques de vérification continue de l'identité, d'accès au moindre privilège, d'application dynamique des politiques et de micro-segmentation, afin de minimiser le risque de brèches internes et externes.

2. **Sécurisez l'ensemble du cycle de vie des données grâce à des contrôles intégrés.** Exigez que toutes les données, qu'elles soient collectées, stockées, transmises, traitées ou éliminées, soient protégées par des mesures de sécurité à plusieurs niveaux. Cela inclut le chiffrement au repos et en transit, des contrôles d'accès stricts, un stockage immuable et le strict respect de réglementations telles que le RGPD et la norme ISO/IEC 27001:2022. Toute lacune au cours d'une étape peut compromettre l'ensemble du système.

3. **Renforcez les modèles d'IA face aux menaces émergentes.** Établissez des protocoles pour vous défendre contre les attaques spécifiques visant l'IA, telles que l'empoisonnement des données, les exploits par porte dérobée, les entrées contradictoires, l'inversion de modèle et l'exploitation des biais. Intégrez un entraînement contradictoire, un filigranage des modèles et des tests réguliers par une « équipe rouge » pour identifier et corriger les vulnérabilités avant le déploiement.

4. **Intégrez la sécurité dès la conception dans les initiatives d'IA.** Insistez pour que chaque nouveau projet d'IA ou de données intègre la sécurité et la confidentialité dès le départ. Exigez que les quipes interfonctionnelles (notamment chargées des données, de l'informatique, de la conformité et de la sécurité) travaillent ensemble pour garantir que les contrôles techniques et de gouvernance sont intégrés au développement et aux opérations des modèles d'IA.

5. **Investissez dans des capacités de cybersécurité proactives basées sur l'IA pour les entreprises.** Allouez des ressources pour développer et déployer des solutions de cybersécurité intelligentes et adaptatives alimentées par l'IA. Cela devrait inclure la détection automatique des menaces, des outils d'évaluation des risques et une surveillance en temps réel pour suivre le rythme de l'évolution des méthodes d'attaque basées sur l'IA. Favorisez la collaboration avec les pairs du secteur et les partenaires du secteur public afin de garder une longueur d'avance sur les menaces émergentes.

Chapitre cinq

La gouvernance des données : la clé de voûte d'une IA d'entreprise fiable

Avant que l'IA puisse penser, elle doit se fier aux informations sur lesquelles elle repose. La gouvernance est ce qui rend cela possible. C'est la discipline qui transforme le contenu dispersé en un actif cohérent, conforme et utilisable, capable d'alimenter des systèmes intelligents en toute sécurité sans compromettre la sécurité ou l'intégrité.

La gestion des informations d'entreprise considère la gouvernance comme un principe de fonctionnement, et non comme une liste de contrôle. Elle repose sur quatre piliers interdépendants : les métadonnées, les autorisations et le contrôle d'accès, la conservation et la gestion du cycle de vie, et l'auditabilité. Chacun définit le comportement des données tout au long de leur durée de vie et, ensemble, ils constituent l'épine dorsale d'un renseignement fiable. Dans ce chapitre, nous examinerons chacun de ces piliers et leur relation avec une IA optimisée, conforme et sécurisée.

> *Forrester prévoit que les dépenses liées aux logiciels de gouvernance de l'IA quadrupleront d'ici 2030.* [38]

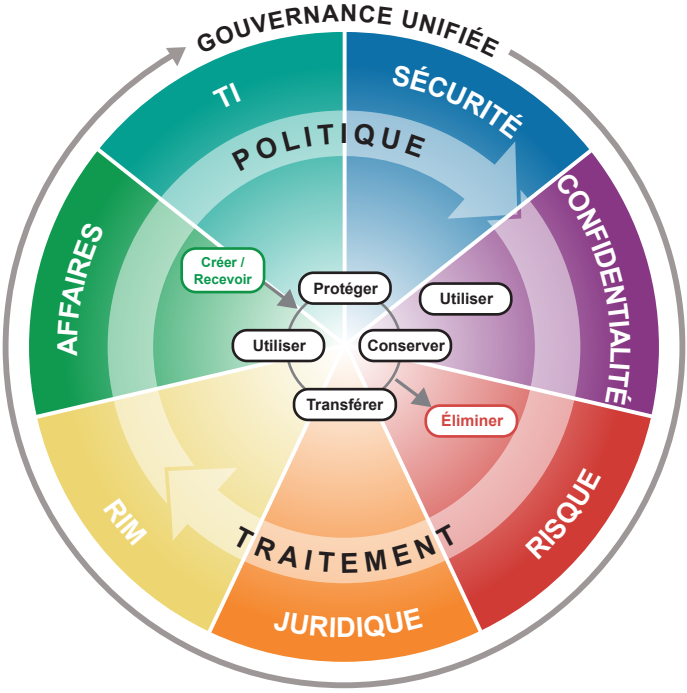
Une bonne gouvernance, c'est une bonne affaire

La gouvernance de l'information est la pratique qui consiste à mettre en œuvre des politiques, des processus et des contrôles pour gérer les informations conformément aux exigences réglementaires, juridiques, de gestion des risques, environnementales et opérationnelles. L'augmentation du volume d'informations de l'entreprise s'accompagne d'un besoin de gouvernance numérique afin de garantir que ces informations sont gérées, sécurisées et consultables. Du point de vue technologique, la gouvernance repose sur la gestion efficace des informations tout au long de leur cycle de vie, depuis leur création, leur capture et leur classification jusqu'à leur archivage ou leur suppression à long terme.

Pour être efficaces, les programmes de gouvernance de l'information exigent que les entreprises trouvent un équilibre entre leurs besoins et priorités afin de limiter les risques juridiques et commerciaux et les coûts liés à la gestion des informations structurées et non structurées. Pour qu'une stratégie de gouvernance de l'information soit efficace, les ressources et les parties prenantes clés doivent être identifiées, responsabilisées et soutenues. Les politiques doivent être intégrées dans des processus pertinents, l'éducation et la formation doivent être dispensées à tous les employés, l'infrastructure technologique doit être optimisée, et les solutions appropriées doivent être mises en œuvre pour soutenir des opérations sûres et fiables.

Dans l'article suivant, ASR Nederland montre à quel point une bonne gouvernance est bénéfique pour son entreprise, en lui permettant de se conformer aux réglementations et en lui fournissant un avantage stratégique grâce à un meilleur service client.

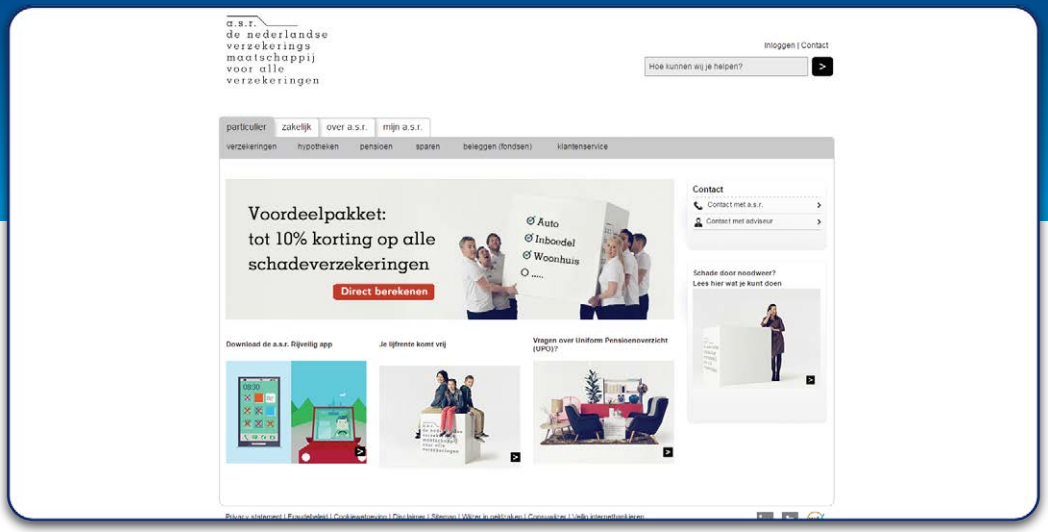
Équilibrer la valeur, le risque et le coût



Modèle de référence sur la gouvernance de l'information [39]

Étude de cas

ASR Nederland



ASR Nederland

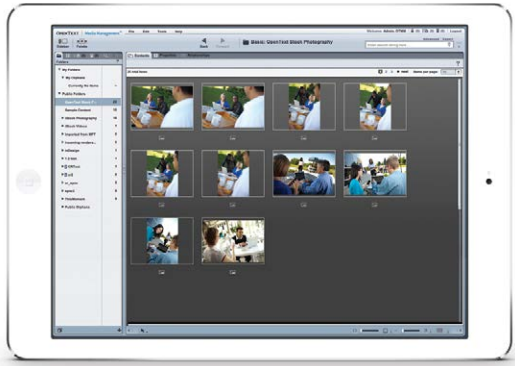
L'une des principales activité commerciales d'ASR est l'assurance invalidité. Auparavant, ce processus de réclamation se faisait par support papier. Les informations médicales et techniques étaient conservées dans un seul dossier accessible au personnel non qualifié, ce qui a entraîné une non-conformité avec la loi néerlandaise sur la protection de la vie privée. En outre, ASR nécessitait un espace de stockage important pour stocker des dossiers toujours plus nombreux. ASR a compris le besoin d'avoir une solution qui améliorerait les processus d'entreprise, qui permettrait la collaboration entre les départements, qui réduirait les coûts dans l'ensemble de l'organisation et qui n'autoriserait que l'accès autorisé aux informations afin de se conformer aux réglementations.

En combinant la modélisation des processus métier avec des solutions d'amélioration opérationnelle, ASR a réussi à moderniser les processus existants tout en s'adaptant aux changements législatifs. Par exemple, les informations médicales et techniques relatives aux demandes d'invalidité sont désormais séparées et accessibles uniquement au personnel qualifié, ce qui permet à ASR de se conformer à la législation sur la protection de la vie privée. De plus, l'ensemble du processus de gestion des réclamations peut être mesuré pour donner à la direction une visibilité sur les processus. L'environnement flexible propose une nouvelle méthode de référence afin de suivre les activités commerciales dans de nombreuses divisions.

Cette solution permet à ASR de disposer d'un système standard de traitement des demandes d'indemnisation à l'échelle de l'entreprise, ce qui a permis d'améliorer considérablement l'efficacité interne et d'accroître la productivité. Les employés traitent désormais 80 % des demandes dans les temps impartis, ce qui a permis de réduire de 25 % l'équipe chargée du traitement des demandes, et les coûts des services et des indemnités ont été considérablement réduits – ce qui permet à ASR de proposer de nouveaux produits plus rapidement, de se conformer aux réglementations et d'offrir un meilleur service à la clientèle.

Maintenant que nous avons vu les avantages de la gouvernance des données pour l'entreprise, examinons les quatre principaux piliers d'une gouvernance des données solide présentés au début de ce chapitre.

Pilier 1 : Les métadonnées : le contexte derrière chaque décision



Les métadonnées dans un système de gestion des actifs numériques

Les métadonnées sont l'ADN des informations numériques : le contexte caché qui indique aux systèmes ce qu'est une information, d'où elle vient et comment elle doit être utilisée. Elles associent le contenu à l'objectif commercial et transforment les données brutes en informations consultables, gouvernables et enseignées.

L'information entre dans l'entreprise par de nombreuses portes. Certains sont numériques, créés par des personnes utilisant des traitements de texte, des feuilles de calcul, des logiciels de CAO ou des clients de messagerie. Certaines trouvent leur origine dans les systèmes commerciaux, générées par les systèmes de planification des ressources d'entreprise (PRE), la gestion de la relation client (CRM), ou dans des bases de données avec des schémas et des structures relationnelles définis.

Les autres contenus sont capturés à partir de sources analogiques, sous forme de scanners. Ensuite, il y a les données des machines provenant des capteurs, des journaux et de la télémétrie, ainsi que le contenu Web et social provenant des intranets, des outils de collaboration et des portails. Les entreprises produisent également des données multimédia (vidéos de formation, ressources marketing et réunions enregistrées) qui ont toutes une valeur opérationnelle et juridique.

La gestion de cette diversité nécessite une couche de contrôle. Les métadonnées (classification, balises de rétention, provenance et sensibilité) constituent cette couche de contrôle. Elles permettent l'attribution automatique des autorisations, la recherche ciblée, le contrôle des versions et l'application des dossiers. C'est également le fondement d'une IA d'entreprise responsable : sans métadonnées, un modèle IA ne peut pas faire la distinction entre un brouillon et une version finale, ou entre une brochure publique et un fichier client privilégié.

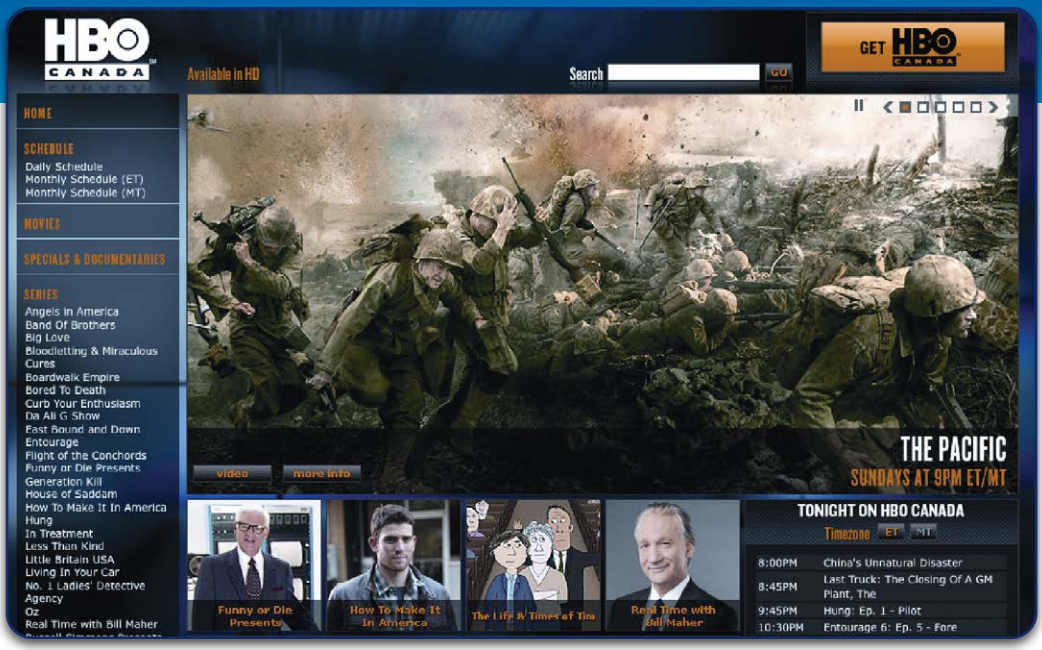
Les métadonnées fournissent le contexte essentiel : qui a créé quoi, quand cela a été modifié, d'où cela vient et dans quelle mesure cela est sensible. Ces informations donnent du sens au contenu brut et aident les utilisateurs et les systèmes intelligents à comprendre ce qui est fiable, ce qui peut être partagé et ce qui doit être protégé.

Sans métadonnées unifiées, l'apprentissage de l'IA n'est pas fiable ou dangereux. LA GIE fournit le cadre permettant d'associer la gouvernance directement aux modèles d'information, en veillant à ce que l'automatisation et l'IA respectent les limites commerciales, juridiques et éthiques qui définissent déjà les données fiables.

Les métadonnées ne sont pas une étiquette statique, c'est un cadre évolutif pour l'application des politiques et le raisonnement automatique. À mesure que l'IA évolue, les métadonnées deviennent le tissu conjonctif entre les données gouvernées et l'action intelligente. Découvrez comment HBO s'appuie sur les métadonnées pour consolider et gérer ses actifs tout au long de leur cycle de vie.

Étude de cas

HBO



Le système de gestion des médias de HBO

HBO est la chaîne de télévision premium la plus populaire des États-Unis. Elle propose du contenu multimédia numérique riche, des films à succès, des programmes originaux innovants, des documentaires audacieux, des concerts et des matchs de boxe. HBO a cherché une solution qui lui permettrait d'accéder facilement au contenu numérique et de le partager, à la fois avec HBO et avec la grande famille Time Warner. Les exigences relatives à la fonctionnalité globale du système et à l'expérience utilisateur impliquaient que le système gère de gros volumes de contenu, ainsi que des bases de données, des flux de traitement et des cas d'utilisation disparates pour chacune des entreprises.

La mise en œuvre de HBO Media Management a englobé toutes les photographies numériques de HBO dans des domaines tels que le marketing, les promotions, la publicité et les ventes. Ces ressources peuvent inclure des photos ou des films comme une galerie de photos professionnelles de qualité de célébrités de HBO.

Leur stratégie globale consistait en partie à garantir une gestion prudente des métadonnées. Les actifs sont étiquetés avec les métadonnées correspondantes, telles que les informations contractuelles, le plus tôt possible afin de garantir que les métadonnées accompagnent l'actif tout au long de son cycle de vie. Ce processus de méta-balisage est appliqué par un composant intégré de flux de traitement. Le système de gestion des actifs numériques de HBO est accessible à tous les bureaux régionaux et contient actuellement plus de 325 000 actifs.

> *Si la gouvernance définit les règles, les autorisations les appliquent, une décision à la fois.*

Pilier 2 : Autorisations et contrôle d'accès : qui peut voir quoi, quand et pourquoi

Les autorisations définissent les limites de la confiance. Elles déterminent qui peut consulter, modifier ou partager des informations, et selon quelles conditions. Depuis des décennies, ces principes protègent les données personnelles et professionnelles. À l'ère de l'IA, ils doivent faire face à une nouvelle urgence. Chaque décision prise par un système intelligent dépend de l'accès : quelles données il peut consulter, quelles leçons il peut tirer et quelles actions il est autorisé à effectuer.

Dans un environnement d'information d'entreprise, les autorisations ne sont pas de simples commutateurs informatiques, elles constituent un niveau d'application de la gouvernance. Le contrôle des versions, les dossiers des flux de travail, la mise en attente des documents et la publication sélective en dépendent. Les modèles d'autorisation efficaces réglementent non seulement ce que les utilisateurs peuvent faire, mais aussi quand et pourquoi. Un document qui peut être modifié aujourd'hui peut être verrouillé demain dans le cadre d'un processus réglementé ou d'une mise en attente juridique. Ce contrôle dynamique garantit la traçabilité et la fiabilité des informations, même lorsqu'elles traversent des cycles de vie complexes et des environnements collaboratifs.

Autorisation et contrôle d'accès

Les systèmes GIE modernes atteignent cette précision grâce à des autorisations granulaires. Chaque objet (document, dossier, flux de traitement ou image) possède son propre profil de sécurité, qui définit l'accès de chaque utilisateur et de chaque groupe au sein du système. À l'échelle de l'entreprise, où les utilisateurs peuvent se compter par centaines de milliers, ces modèles peuvent se traduire par des milliards de combinaisons d'autorisations uniques. Pourtant, cette complexité est indispensable. Sans la capacité d'attribuer la sécurité au niveau le plus précis possible, un système d'information ne peut pas vraiment être considéré comme sûr. C'est cette flexibilité qui permet aux entreprises d'imiter les contrôles physiques d'un espace de travail sécurisé, numériquement et à grande échelle.

À mesure que l'IA devient un autre « utilisateur » du système, ces mêmes structures d'autorisation doivent s'étendre aux agents intelligents. Si un document est confidentiel, l'IA doit également le savoir. Les autorisations ne sont plus simplement une question de contrôle ; elles sont une question de confiance, qui permet à chaque personne et à chaque système d'interagir avec les informations de manière ciblée, dans des limites définies et en toute responsabilité. C'est ainsi que les entreprises protègent la vie privée, préservent leur avantage concurrentiel et veillent à ce que l'IA fonctionne en toute sécurité dans les zones où elle est autorisée à apprendre.

L'étude de cas ci-dessous, qui concerne une banque d'investissement européenne, illustre une utilisation efficace des autorisations pour classer les documents entre les différents sites afin d'atteindre les objectifs opérationnels et de gouvernance.

Étude de cas

Une banque européenne

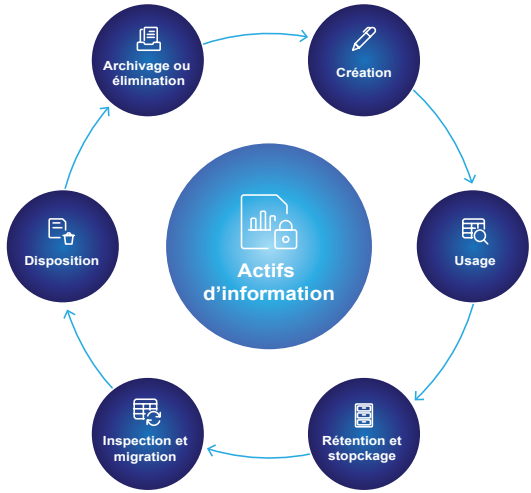
Une banque d'investissement en Europe finance des investissements de capitaux conformes aux objectifs politiques de l'Union européenne – l'infrastructure littérale d'une Europe plus intégrée. Avec des activités réparties dans 150 pays en dehors de l'UE, l'accès à distance sécurisé et efficace aux documents n'est pas une simple commodité – c'est essentiel. Pour y parvenir, la banque a mis en place un système GIE dans le cadre d'un effort plus large de modernisation informatique visant à transformer tous les principaux processus de la banque : emprunt, prêt et administration. Le système était entièrement intégré à l'écosystème informatique de la banque afin que le contenu, les données et les flux de traitement puissent être transférés facilement d'un système à l'autre, garantissant ainsi la cohérence et la conformité de toutes les opérations.

La gouvernance est au cœur de ce système. La banque d'investissement a développé une taxonomie à l'échelle de la banque qui définit non seulement la manière dont le contenu est classé, mais aussi la manière dont il s'aligne sur les processus commerciaux et les cadres réglementaires. Basée sur les meilleures pratiques internationales, notamment la méthodologie DIRKS et les normes ISO 15489, cette taxonomie est associée à un modèle de contrôle d'accès sophistiqué qui s'applique aux plus hauts niveaux de classification. Ensemble, ces modèles forment un cadre de gouvernance dynamique : la taxonomie indique quelles informations existent et où elles appartiennent, tandis que le modèle d'autorisations détermine qui peut y accéder, dans quelles conditions et dans quel but. Le résultat est une carte de connaissances numérique qui reflète la structure, les responsabilités et les droits décisionnels de l'institution.

Cette architecture d'information disciplinée constitue désormais la base de l'activation de l'IA. Grâce à une taxonomie cohérente et à des autorisations détaillées, l'entreprise peut entraîner les outils d'intelligence artificielle à récupérer, résumer et classer des documents en toute sécurité, en sachant que chaque action entreprise par un agent intelligent est conforme aux mêmes règles d'accès et de conformité qu'un utilisateur humain. La gouvernance garantit que l'IA ne se contente pas d'automatiser les tâches, mais qu'elle fonctionne dans les mêmes limites de confiance que celles qui définissent les flux de traitement humains de la banque.

Les résultats valident l'approche. Deux mois après le lancement, le taux d'adoption par les utilisateurs était supérieur de 20 % aux prévisions, 100 % des données vitales relatives aux nouvelles opérations de prêt et d'emprunt étant prises en charge par le système. En quelques semaines, le référentiel contenait plus de 600 000 documents, soit une augmentation d'environ 100 000 par semaine. Ce succès a démontré que lorsque la gouvernance, la taxonomie et le contrôle d'accès fonctionnent ensemble, ils ne ralentissent pas l'innovation – ils la rendent évolutive.

Pilier 3 : Rétention et gestion du cycle de vie : savoir quand conserver et quand lâcher prise



La bonne gouvernance garantit la sécurité, la conformité et la continuité des activités

La gouvernance de l'information n'est pas qu'une question de stockage, c'est une question de gestion. Chaque élément de contenu a une vie : création, utilisation, révision, conservation et élimination éventuelle. C'est en gérant ce cycle de vie que les entreprises restent conformes, efficaces et durables.

Les informations ou dossiers réglementés proviennent des quatre coins de l'entreprise : systèmes PRE et CRM, courriels, documents, papier scanné, télémétrie, appareils médicaux et même systèmes de maintenance aéronautique. La première étape de la gouvernance est la capture : transmettre ces informations par le biais de canaux contrôlés tels que les salles de courrier numériques, les connecteurs système ou les API. Chaque enregistrement doit arriver avec ses métadonnées, son horodatage et sa provenance intacts pour garantir son authenticité et sa légitimité juridique. La gouvernance ne commence pas lorsque les informations sont stockées, mais au moment où elles entrent dans le système, lorsque la confiance est créée pour la première fois.

Une fois capturés, les dossiers sont distribués dans des environnements de stockage à plusieurs niveaux qui reflètent leur objectif et leur profil de risque. Les systèmes opérationnels gèrent les documents actifs, les référentiels de gestion de contenu assurent le contrôle des versions, la classification et la conservation, et les archives immuables préservent les communications et les preuves à des fins juridiques ou réglementaires. Dans les environnements analytiques, les données tokénisées peuvent être symbolisées ou masquées pour protéger la confidentialité tout en permettant d'obtenir des informations. Les archives à long terme (sur cassette, dans un entrepôt de stockage d'objets ou dans des clouds souverains) sont conservées de manière non effaçable lorsque la loi l'exige.

Une plateforme GIE intègre des politiques de conservation directement dans les systèmes sur lesquels réside le contenu. Cela garantit que le même document qui soutient une décision commerciale d'aujourd'hui pourra être archivé demain, ou automatiquement supprimé à l'expiration de sa valeur légale ou opérationnelle.

Les mêmes principes qui régissent les dossiers des entreprises s'appliquent désormais à l'intelligence artificielle. Alors que les systèmes d'IA génèrent, consomment et tirent des leçons du contenu de l'entreprise, leurs entrées et sorties doivent être traitées avec la même rigueur que les données réglementées. Chaque interaction du modèle devient son propre enregistrement, soumis à la capture, à la classification, à la conservation et à l'auditabilité. La gouvernance garantit que l'IA apprend auprès de sources fiables, agit dans des limites définies et produit des résultats explicables, défendables et conformes à la politique de l'entreprise. Ainsi, les disciplines qui ont renforcé la confiance dans la gouvernance des données deviennent les garants d'un renseignement responsable.

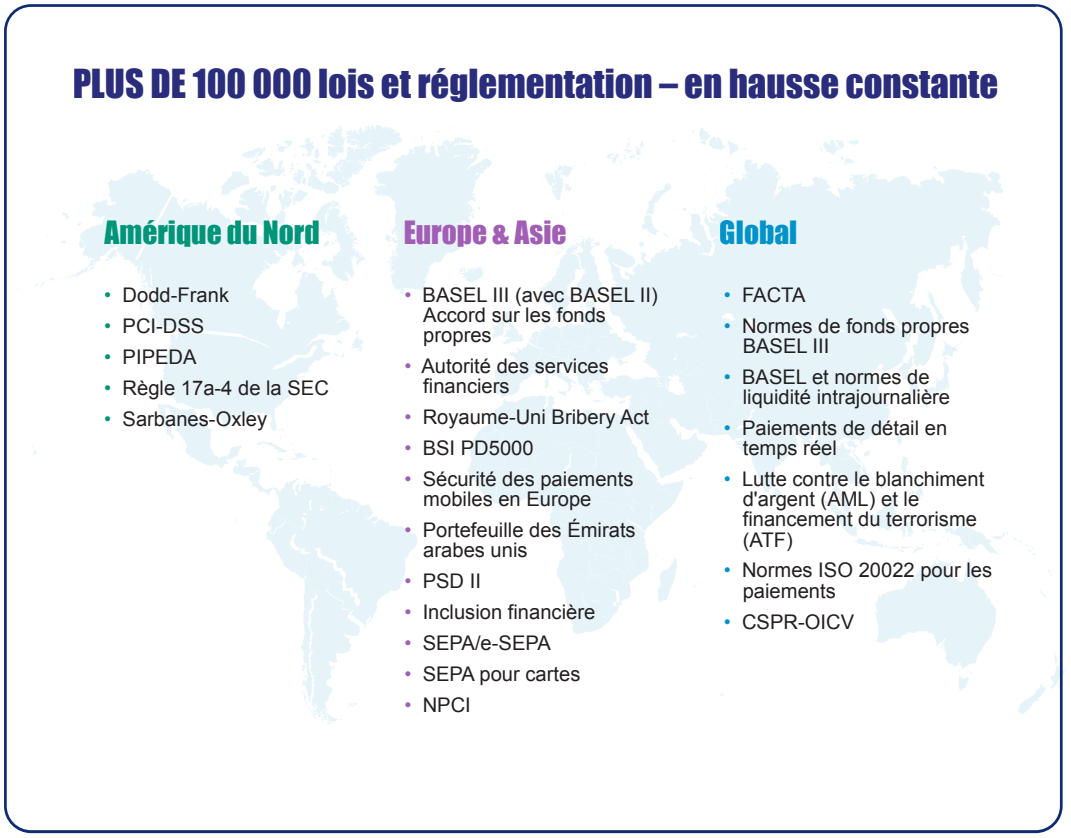
Pilier 4 : L'auditabilité : la preuve que la gouvernance fonctionne

Dans la gestion traditionnelle des dossiers, l'auditabilité impliquait des journaux, des historiques de versions et des traces écrites. À l'ère de l'IA, cela signifie également la transparence des modèles, c'est-à-dire la compréhension des informations qui ont façonné un résultat.

L'auditabilité doit être intégrée au cycle de vie du contenu. Chaque document, transaction et événement système contient un historique traçable des modifications et des approbations. Lorsqu'il est étendu à l'IA, ce même principe fournit des explications, en indiquant non seulement ce qu'un modèle a décidé, mais aussi quelles données ont contribué à cette décision. C'est cette visibilité qui transforme la gouvernance en confiance. L'auditabilité garantit aux régulateurs, aux dirigeants et au public que l'automatisation fonctionne dans des limites définies. Il transforme la conformité d'un processus réactif en une norme vérifiable pour un renseignement responsable.

Ces fonctionnalités de gouvernance sont intégrées à une plateforme GIE dans le cloud. Avec l'évolution de l'IA, la gouvernance doit passer avant tout, car elle définit les règles d'engagement entre les personnes, les données et les systèmes intelligents. Les métadonnées fournissent la carte; les autorisations définissent l'accès; la gestion du cycle de vie garantit l'équilibre; et l'auditabilité prouve la responsabilité.

Sans ces bases, l'IA ne peut que deviner. Avec ces piliers, elle fait partie d'un écosystème d'information discipliné, qui apprend, raisonne et agit dans les limites nécessaires pour garantir la sécurité, la légalité et l'adaptation des informations à l'humain.



Pressions réglementaires mondiales et régionales [40]

Un paysage complexe de gouvernance

Sur le marché mondial actuel, le paysage réglementaire est complexe, en particulier pour les entreprises internationales. Les entreprises sont soumises à des réglementations et normes spécifiques à leur secteur, ainsi qu'à des réglementations régionales ou nationales. Selon ces réglementations, elles sont tenues responsables de leurs actes et doivent être en mesure d'accéder à des années de données historiques pour répondre à tout moment à des demandes d'informations.

La relation entre conformité et gouvernance est réciproque. La conformité est le moteur de la gouvernance des informations, et la gouvernance des informations, en retour, peut simplifier la conformité. Face à l'augmentation des volumes de données, il est absolument nécessaire de mettre en place des programmes de gouvernance pour aider les entreprises à bénéficier d'une meilleure gestion de leurs informations. Les entreprises qui mettent en œuvre une GIE en tant que plateforme de gouvernance réalisent les opportunités qu'elle leur offre pour conduire la transformation de l'entreprise efficacement grâce à l'optimisation des informations et de l'IA.

La conformité a de multiples facettes

Conformité, souveraineté et forme d'une gouvernance moderne

La souveraineté des données est passée d'une note de bas de page sur la conformité à un principe de conception. Elle définit désormais où se trouvent les données, qui peut y accéder et sous quelle juridiction relèvent ces actions. Dans un monde piloté par l'IA, cela est très important : les modèles formés ou hébergés dans une région peuvent toujours être régis par les lois d'une autre. Le résultat est que la souveraineté n'est plus une abstraction légale, c'est une contrainte architecturale. Chaque choix de stockage, chaque API et chaque ensemble de données de formation doivent désormais tenir compte de la géographie réglementaire concernée.

Les lois sur la protection de la vie privée et réglementation régionale

L'Europe a donné le ton au niveau mondial avec le règlement général sur la protection des données (RGPD). Cela a transformé les flux de données transfrontaliers d'une hypothèse technique en un défi d'ingénierie juridique. Le GDPR a codifié les principes de légalité, de limitation des finalités, de minimisation et de responsabilité, en exigeant un consentement clair, des évaluations d'impact et des droits pour les personnes concernées. Son application a modifié la façon dont les entreprises conçoivent leurs systèmes : les inventaires de données, les flux de travail basés sur les métadonnées et les politiques de suppression automatisées sont désormais des fonctions de gouvernance de base, et non des contrôles facultatifs.

La loi européenne sur les données étend ces idées à la mobilité dans le cloud. Les fournisseurs doivent désormais garantir l'interopérabilité et permettre aux clients de quitter librement les environnements cloud, sans blocage ni frais de transfert excessifs. Pour les architectes, cela signifie construire en tenant compte de la portabilité : normes ouvertes, formats réversibles et indépendance du cloud dès la conception. En Europe, la souveraineté est légiférée.

De l'autre côté de l'Atlantique, les États-Unis sont en train de mettre en place une norme fédérale de facto, État par État. Plus de vingt États appliquent désormais leurs propres lois complètes sur la protection de la vie privée, chacune définissant différemment le consentement, les données sensibles et les droits des utilisateurs. Cette mosaïque exige des règles en tant que code : des règles automatisées qui s'adaptent aux nuances juridictionnelles et garantissent que la bonne loi s'applique au bon dossier, au bon utilisateur ou à la bonne transaction. Le CLOUD Act complique encore les choses en autorisant les autorités américaines à accéder aux données détenues par des fournisseurs basés aux États-Unis, même lorsqu'elles sont stockées à l'étranger, obligeant ainsi les entreprises internationales à réfléchir sérieusement au contrôle contractuel et à la souveraineté du stockage.

Le modèle multicouche du Canada

Le Canada aborde la souveraineté par le biais d'une responsabilité à plusieurs niveaux. Au niveau fédéral, la LPRPDE, ou Loi sur la protection des renseignements personnels et les documents électroniques, définit les bases d'un traitement responsable des informations personnelles, en autorisant les transferts transfrontaliers tout en garantissant que les entreprises restent responsables de la protection de bout en bout. Son prochain remplacement, la Loi de 2022 sur la mise en œuvre de la Charte du numériquee (projet de loi C-27), introduit la Loi sur la protection de la vie privée des consommateurs, un tribunal de protection des données, et la Loi sur l'intelligence artificielle et les données, conçues pour régir le développement et le déploiement responsables de l'IA.

Au niveau provincial, la conformité devient plus précise. Les réformes de la FOIPPA (Freedom of Information and Protection of Privacy Act) de la Colombie-Britannique ont assoupli les restrictions de résidence pour les données publiques, tandis que la Loi sur la protection des renseignements personnels sur la santé (LPRPS) continue à appliquer des normes strictes en matière d'information sur la santé en Ontario. Les régulateurs financiers, tels que le BSIF ou le Bureau du surintendant des institutions financières, ont fait de la localisation des données et de la supervision du cloud des responsabilités au niveau du conseil d'administration, conformément à la directive B-10. Le message est constant : la souveraineté au Canada est à la fois pratique et provinciale, ce qui exige de cartographier soigneusement où se trouvent les données et qui peut y accéder.

Conformité mondiale et règles spécifiques au secteur

Au-delà de l'Amérique du Nord et de l'Europe, les pressions en matière de souveraineté des données sont mondiales. La loi chinoise sur la protection des informations personnelles (PIPL) impose des évaluations de sécurité explicites pour les transferts transfrontaliers de « données importantes ». La loi indienne sur la protection des données personnelles numériques (DPDP) ajoute des dispositions de type localisation et de nouvelles conditions de transfert susceptibles d'influencer le lieu et le mode de fonctionnement des charges de travail liées à l'IA. Chaque règlement renforce les attentes en matière de transfert légal, de consentement explicite et de discipline en matière de rétention.

Les réglementations du secteur amplifient ces exigences. La loi américaine HIPAA, ou Health Insurance Portability and Accountability Act, est un cadre qui régit les dossiers médicaux électroniques avec un contrôle d'accès, un cryptage et une notification des violations stricts. Le 21 CFR Part 11 de la FDA (Food and Drug Administration) définit les normes relatives à la fiabilité des enregistrements et des signatures électroniques dans les environnements industriels et cliniques réglementés. La FTC, ou Federal Trade Commission, fait preuve de « diligence raisonnable » en matière de sécurité des données des consommateurs, tandis que la FAA, ou Federal Aviation Administration, définit les exigences d'authenticité et de traçabilité pour les dossiers de maintenance numériques dans l'aviation. Toutes ces lois et réglementations renforcent une vérité commune : les données réglementées doivent être capturées, conservées et auditables tout au long de leur cycle de vie.

La souveraineté et IA

Pour l'intelligence artificielle, ces lois se traduisent par des limites opérationnelles et des choix de conception. L'IA d'entreprise ne peut pas apprendre de ce qu'elle ne peut pas légalement voir. Les clouds souverains, conçus pour localiser le stockage, le traitement et l'accès, sont en train de devenir la réponse architecturale à la fragmentation réglementaire. Ils permettent aux entreprises de déployer l'IA là où se trouvent les données, en respectant les limites juridictionnelles tout en maintenant le contrôle nécessaire à la conformité et à la confiance.

Au fur et à mesure que les modèles IAE deviendront plus agentiques, la souveraineté définira leur périmètre : ce qu'ils sont autorisés à lire, ce qu'ils peuvent conserver et comment leurs actions sont enregistrées et expliquées. La conformité n'est plus une question d'enregistrements statiques, mais de systèmes dynamiques qui pensent, apprennent et agissent sous surveillance légale. Une plateforme de gestion des informations d'entreprise dotée d'une gouvernance intégrée est désormais le système d'exploitation du renseignement lui-même.

La gouvernance en tant que système d'exploitation de la confiance

Dans un monde où les informations traversent les frontières, les clouds et les algorithmes, la gouvernance définit les règles d'engagement. Cela garantit que les données restent précises, traçables et défendables, peu importe où elles voyagent ou comment elles sont utilisées.

Une gouvernance efficace ne se limite pas à de la documentation. Elle exige le soutien des dirigeants, des processus rationalisés, l'application automatisée des politiques et une sécurité centrée sur l'identité. Cela exige que chaque action sur les données, de leur capture à leur élimination, soit visible, auditable et conforme aux normes légales et éthiques.

Les environnements de développement modernes de gestion de l'information intègrent désormais ces contrôles directement dans les opérations quotidiennes. Les métadonnées, les autorisations et la conservation ne sont pas une question secondaire ; il s'agit d'une logique intégrée qui garantit l'honnêteté des systèmes et la responsabilité de l'IA. En traitant l'information comme un actif géré - avec sa provenance, sa finalité et son cycle de vie - les organisations transforment la gouvernance d'un coût de fonctionnement en une source d'avantage concurrentiel.

En fin de compte, c'est grâce à la gouvernance que les entreprises peuvent se fier à leurs renseignements. Cela fait le lien entre l'éthique de la façon dont nous gérons les informations et les mécanismes selon lesquels l'IA en tire des leçons. Lorsqu'elle est bien menée, la gouvernance ne ralentit pas l'innovation, elle la rend durable.

Nous allons parler de la gouvernance de l'IA plus en détail dans le chapitre suivant.

Télécharger The Fast Five

1. **Faites de la gouvernance un mandat d'entreprise.**
   Mettez en place un conseil de gouvernance interfonctionnel composé de responsables commerciaux, informatiques, juridiques et de conformité. Donnez au service informatique le pouvoir de définir les politiques relatives aux données à l'échelle de l'entreprise, d'approuver les cas d'utilisation de l'IA et de contrôler le respect des règles. La gouvernance n'est pas un projet informatique, c'est une discipline de gestion.

2. **Rendez opérationnels les autorisations et le contrôle d'accès.**
   Passez des autorisations statiques basées sur les rôles à un accès dynamique régi par des politiques. Cartographiez les personnes autorisées à voir ou à utiliser des informations spécifiques, et étendez ces mêmes commandes aux systèmes d'IA. Traitez chaque interaction avec l'IA comme un événement régi, avec des pistes d'audit, des dates d'expiration et une responsabilité explicite.

3. **Cartographiez et classez les actifs de données critiques.**
   Réalisez des inventaires des données d'entreprise afin de localiser les informations sensibles, réglementées et de grande valeur. Utilisez les outils GIE pour étiqueter le contenu à l'aide de métadonnées (propriété, sensibilité et rétention) afin qu'il puisse être utilisé en toute sécurité pour la formation, l'automatisation et les analyses liées à l'IA.

4. **Intégrez la conformité et la souveraineté à l'architecture.**
   Tenez compte de la complexité juridictionnelle dès le départ de la conception. Choisissez des configurations cloud souveraines ou régionales où la résidence des données est importante. Automatisez la conformité grâce aux métadonnées et aux politiques sous forme de code, afin que les règles concernant les lieux où les données peuvent être stockées ou déplacées soient appliquées dès la conception, et non par un audit.

5. **Gérez l'IA comme vous gérez les données.**
   Traitez les modèles comme des actifs gérés avec les mêmes attentes que les données : provenance documentée, contrôle du cycle de vie et gouvernance du recyclage. Exigez que chaque initiative d'IA fasse la preuve d'une utilisation légale des données, de décisions explicables et d'un retour sur investissement mesurable avant d'être déployée à grande échelle.

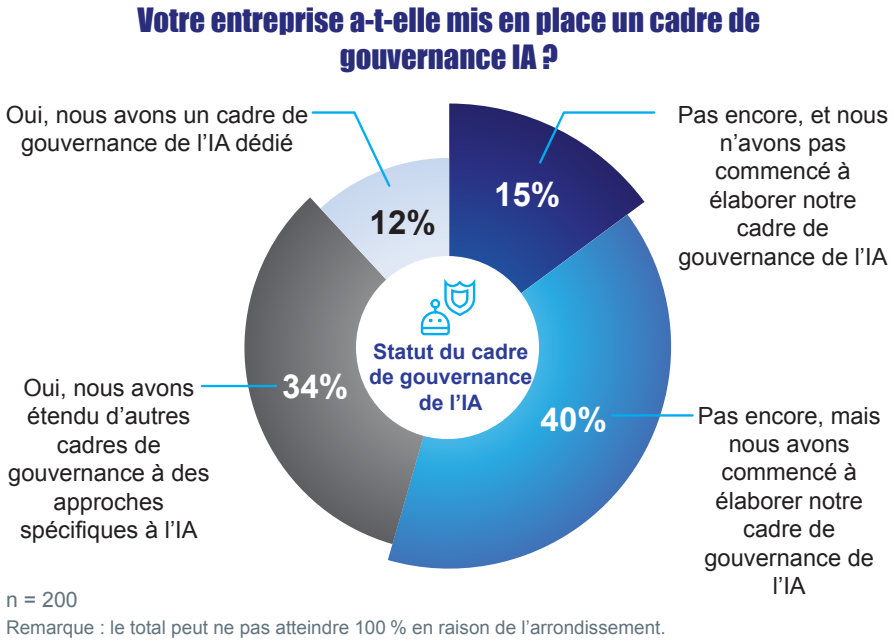
Chapitre six

La gouvernance de l'EAI

Comme nous l'avons vu dans le chapitre précédent, les progrès technologiques s'accompagnent du besoin d'une gouvernance et de contrôles efficaces. Si la gouvernance des données est plus mature dans son histoire et son évolution, le besoin de gouvernance de l'IA rattrape rapidement son retard. La gouvernance de l'IA fournit les politiques, les processus et les contrôles qui garantissent que les technologies IAE sont conformes aux objectifs organisationnels et aux exigences réglementaires.

Dans ce chapitre, nous allons explorer comment la gouvernance transforme l'IA à partir d'une capacité technique en un actif stratégique de confiance. Nous explorerons l'importance de la gouvernance de l'IA dans les secteurs privé et public en mettant l'accent sur le champ d'application, l'éthique, la conformité, la gestion des risques et la responsabilité.

Selon Gartner, seulement 12 % des entreprises ont mis en œuvre un cadre de gouvernance dédié à l'IA, tandis que 55 % déclarent ne pas l'avoir encore fait. [41]



Enquête Gartner auprès des responsables de service informatique, des données et de l'analytique sur la stratégie en matière d'intelligence artificielle [42]

À mesure que l'IA est intégrée dans tous les secteurs de l'entreprise, la gouvernance est devenue son fondement essentiel. Une gouvernance efficace de l'IA assigne les responsabilités, définit la supervision et garantit que les systèmes intelligents fonctionnent de manière éthique et transparente. Sans cela, les entreprises risquent de s'exposer à des préjugés, à des violations de la vie privée et à des atteintes à leur réputation. Pourtant, nombreuses sont celles qui rencontrent encore des difficultés, faute d'avoir l'expertise, la coordination et les données unifiées nécessaires pour gérer l'IA à grande échelle.

À l'avenir, la gouvernance déterminera non seulement la manière dont l'IA sera déployée, mais aussi la manière dont elle gagnera la confiance. Les entreprises tournées vers l'avenir alignent déjà leur gouvernance sur l'évolution des réglementations et intègrent dès le départ des pratiques responsables en matière d'IA dans leurs activités.

Dans l'étude de cas suivante, découvrez comment un cabinet de conseil international figure parmi les 12 % de Gartner en matière de gouvernance de l'IA.

Étude de cas

Un cabinet de conseil mondial

Cette entreprise est un leader innovant dans les domaines de la stratégie, de la conception et du développement en ligne et mobile, ainsi que de la cybersécurité. Elle offre des connaissances et des ressources de premier plan provenant du principal cabinet de conseil commercial et technologique mondial. L'entreprise a conscience du point d'inflexion numérique actuel, où l'intelligence artificielle, l'automatisation et les technologies cloud remodèlent les modèles d'entreprise, la dynamique de la main-d'œuvre et même la culture organisationnelle. Voici des extraits d'un entretien avec un analyste technique de premier plan de l'entreprise.

« Parallèlement à la transformation numérique, les données elles-mêmes ont évolué. Il ne s'agit plus uniquement de transactions, mais de contexte. La valeur réside désormais dans les relations entre les données structurées et non structurées : les conversations, les images et les signaux qui donnent un sens à ce qui est mesuré. L'intelligence artificielle et l'analytique permettent d'extraire ce sens à grande échelle, transformant les informations non structurées en informations exploitables. Lorsqu'elles sont combinées sur une plateforme d'information unifiée, les analyses basées sur l'IA exploitent un potentiel exponentiel, révélant des liens et des risques que nous n'avions jamais vus auparavant.

Mais cette opportunité s'accompagne de responsabilités. Alors que l'IA renforce son rôle dans la prise de décision des entreprises, l'importance de la cybersécurité n'a jamais été aussi grande. Chaque système intelligent dépend de données fiables et d'une infrastructure sécurisée. Une solide doctrine de sécurité, qui englobe la gouvernance, la conformité et la défense proactive, permet de sécuriser les données de l'entreprise. Nous sommes conscients que, quelle que soit l'évolution des technologies, les principes fondamentaux restent les mêmes : des environnements de développement clairs, l'application de politiques et une surveillance vigilante, le tout consolidé dans une plateforme GIE.

Alors que les entreprises adoptent des modèles hybrides et multicloud, la question n'est pas seulement de savoir où stocker les données, mais aussi comment les protéger. L'intelligence artificielle amplifie à la fois le pouvoir et le risque de la transformation numérique, et fait de la cybersécurité une garantie technique, mais également le fondement de la confiance dans une entreprise intelligente. »

Quelle est la portée de la gouvernance de l'IAE ?

La gouvernance de l'IA guide la manière dont une entreprise développe, déploie et gère l'IA conformément à ses objectifs stratégiques et à ses obligations réglementaires. En tant qu'extension de la gouvernance d'entreprise et informatique, la gouvernance IAE répond à des défis tels que la supervision des modèles, les biais, la gestion des données, le contrôle des risques de cybersécurité et la conformité. La plupart des entreprises établissent désormais des politiques d'utilisation responsable de l'IA qui intègrent des principes comme l'équité, la transparence et la responsabilité tout au long du cycle de vie de l'IA. Ces garde-fous deviennent essentiels pour garantir une adoption fiable et responsable de l'IA et pour maintenir la confiance du public dans les systèmes d'intelligence modernes.

Les principaux cadres actuels qui guident la gouvernance de l'IAE incluent les principes de l'Organisation de coopération et de développement économiques (OCDE) en matière d'IA, le projet de loi sur l'IA de l'Union européenne, le cadre de gestion des risques liés à l'IA (AI RMF) du National Institute of Standards and Technology (NIST) et les normes de l'Organisation internationale de normalisation (ISO) sur l'IA.

De plus en plus, la gouvernance de l'IAE s'étend au-delà des systèmes immédiats de l'entreprise, en y incluant les modèles et l'infrastructure dont elle dépend. Les nouveaux cadres réglementaires, notamment la loi européenne sur l'IA (2024) et le décret exécutif américain 14110 sur la sécurité de l'IA (2023), font la distinction entre la gouvernance des systèmes d'IA (la façon dont une entreprise gère sa propre utilisation de l'IA) et la gouvernance au niveau des modèles (les obligations des personnes qui développent ou affinent des modèles d'IA à usage général, les « IA Fontière »). Les entreprises sont désormais tenues de faire preuve de diligence raisonnable sur les fournisseurs modèles avant l'intégration (NIST, 2023 ; Commission européenne, 2024). Cela introduit la responsabilité dans l'ensemble de la chaîne d'approvisionnement en IA.

> *L'éthique des données ne se limite pas à la conformité : il s'agit de faire le bon choix, même lorsque la loi ne l'exige pas.* [43]

Garantir une IA éthique et responsable

La gouvernance éthique garantit que les systèmes d'IA sont équitables, transparents et respectueux des droits de l'homme. Bien que le terme « IA éthique » puisse sembler contemporain, ses racines remontent à plusieurs décennies, lors de discussions fondamentales sur l'éthique informatique. Dans son essai historique de 1985, « What Is Computer Ethics ? », Moor a souligné ceci :

> « L'un des problèmes typiques de l'éthique informatique est dû à un vide politique quant à la manière dont la technologie informatique devrait être utilisée. Les ordinateurs nous fournissent de nouvelles capacités qui, à leur tour, nous offrent de nouveaux choix d'action. Souvent, soit il n'existe aucune politique de conduite dans ces situations, soit les politiques existantes semblent inadéquates. L'une des tâches essentielles de l'éthique informatique est de déterminer ce que nous devons faire dans de tels cas, c'est-à-dire de formuler des politiques pour guider nos actions. Bien entendu, certaines situations éthiques nous interpellent en tant qu'individus, et d'autres en tant que société. L'éthique informatique inclut la prise en compte des politiques personnelles et sociales relatives à l'utilisation éthique de la technologie informatique. » [44]

Des écrits ultérieurs ont porté spécifiquement sur l'éthique de l'IA, notamment les « Principes sur l'intelligence artificielle » (2019) de l'OCDE et, plus récemment, la « Recommandation sur l'éthique de l'intelligence artificielle », publiée par l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO) en 2022. Avec 194 États membres à l'ONU, ce dernier ensemble de recommandations constitue le cadre le plus vaste publié à ce jour.

Les recommandations justifient clairement le besoin de directives éthiques :

> « Les systèmes d'intelligence artificielle soulèvent de nouveaux types de problèmes éthiques, notamment leur impact sur la prise de décision, l'emploi et le travail, les interactions sociales, les soins de santé, l'éducation, les médias, l'accès à l'information, la fracture numérique, les données personnelles et la protection des consommateurs, l'environnement, la démocratie, l'État de droit, la sécurité et le maintien de l'ordre, le double usage, les droits de l'homme et les libertés fondamentales, notamment la liberté d'expression, le respect de la vie privée et la non-discrimination. En outre, de nouveaux défis éthiques sont créés par le potentiel des algorithmes d'IA à reproduire et à renforcer les préjugés existants, et donc à exacerber les formes déjà existantes de discrimination, de préjugés et de stéréotypes. » [45]

Les recommandations indiquent en outre que, à mesure que l'IA prend en charge de plus en plus de tâches précédemment exécutées par des êtres humains, son impact sur l'humanité va s'étendre. Elle a le potentiel de modifier profondément la façon dont nous comprenons le monde qui nous entoure, ainsi que notre perception de nous-mêmes. [46]

Les recommandations éthiques en matière d'IA comprennent, sans s'y limiter, les principes suivants :

- **Proportionnalité et ne pas nuire** : Couvrant l'étendue de l'utilisation de l'IA et l'adéquation au contexte d'utilisation
- **Sûreté et sécurité** : Prévention des nuisances, y compris les risques de sécurité
- **Équité et non-discrimination** : Incluant des exigences visant à promouvoir la justice sociale et à garantir l'équité
- **Durabilité** : Incluant une prise en compte des facteurs humains, sociaux, culturels, économiques et des impacts environnementaux sur le développement durable
- **Droit à la vie privée et à la protection des données** : gouverner l'utilisation des données pour l'IA
- **Supervision humaine et détermination** : maintenir le contrôle humain sur l'IA
- **Transparence et explicabilité** : Incluant une compréhension et une explication générales de l'utilisation de l'IA et des données pertinentes dans des cas spécifiques
- **Responsabilité et responsabilisation** : promouvoir les droits de l'homme et les libertés
- **Sensibilisation et littératie** : tirer parti de l'éducation, de la formation et de l'éducation aux médias pour accroître la sensibilisation à l'utilisation de l'IA
- **Gouvernance et collaboration multipartites et adaptatives** : respect des lois internationales et de la souveraineté nationale [47]

Alors que la gouvernance éthique de l'IA institutionnalise le principe « Ne pas nuire », l'intégration de valeurs telles que la non-discrimination, la responsabilité et la transparence est essentielle pour les entreprises et impérative pour les entreprises du secteur public. Pour passer d'une liste de contrôle à un système technique, nous devons considérer l'éthique comme une infrastructure. Cela implique d'intégrer des garde-fous éthiques à chaque phase du cycle de vie de l'IA. En intégrant ces facteurs, l'éthique fait partie intégrante de votre architecture opérationnelle, définissant ce que représente votre organisation et son comportement, et pas seulement ce qu'elle produit. Alors que les entreprises s'orientent vers l'innovation responsable, une IA éthique et responsable est indispensable pour maintenir la croissance et la confiance.

Cadre complet de gouvernance de l'IA

Gérer les risques et préserver la confiance

L'IA présente des risques uniques qui ne sont pas couverts par la gouvernance informatique traditionnelle. C'est pourquoi il est essentiel de renforcer la responsabilisation et le contrôle. Du point de vue de la fiabilité, étant donné que l'IA peut échouer de manière imprévisible, des tests rigoureux sont nécessaires et doivent comprendre de solides protocoles de repli. Du côté de la qualité et des performances, la surveillance continue permet de minimiser les risques. Le plus important, cependant, est de garantir la sécurité, la confidentialité et la sûreté, car les incidents peuvent porter atteinte à la réputation d'une entreprise et éroder la confiance du public. L'intégration de la gestion des risques liés à l'IA à des processus plus larges de gestion des risques d'entreprise (GRE) garantit que les risques liés à l'IA sont traités avec la même rigueur que les risques financiers ou opérationnels.

Les meilleures pratiques suivantes constituent un cadre de gouvernance solide :

Intégration à la gouvernance d'entreprise

Comme indiqué ci-dessus, la gouvernance de l'IAE recoupe les structures existantes (gouvernance d'entreprise, gouvernance informatique et gestion des risques), et nécessite la définition des rôles, des responsabilités et de la supervision à tous les niveaux. Une gouvernance fiable de l'IA est obtenue grâce à une gestion des politiques basée sur les tâches, en tant qu'extension des CABR (Contrôles d'accès basés sur le rôle) existants pour les humains, et désormais pour les agents. L'établissement d'un climat de confiance nécessite des équipes interfonctionnelles composées de technologues, d'éthiciens, de conseillers juridiques et parfois même de clients. L'IA étant une technologie plus récente, le profil de risque doit être considéré comme élevé lors de la quantification de l'ensemble des risques.

Politiques et normes

Pour les entreprises et leurs employés, le fait de disposer de politiques, de codes de conduite et de normes internes clairement définies rend les attentes explicites et applicables. Celles-ci doivent être souvent renforcées et codées dans les règles commerciales des agents d'intelligence artificielle, afin que les décisions autonomes suivent exactement le même cadre éthique pour obtenir les résultats souhaités. Le plus important est d'utiliser des données d'entreprises protégées ou privées et de veiller à ce que les directives relatives à leur utilisation en ce qui concerne les modèles d'IA publics soient simples.

Auditabilité

La gouvernance nécessite une documentation, une journalisation et des pistes d'audit robustes pour tous les systèmes d'IA, à l'appui des examens internes et des audits réglementaires. En définissant ce principe de fonctionnement de base, vous pouvez vous assurer d'être proactif et d'identifier les problèmes avant qu'ils ne surviennent. Nous avons décrit ces aspects de la gouvernance des données dans le chapitre précédent.

Transparence

La transparence est le fondement d'une gouvernance fiable de l'IA : elle garantit que les décisions prises par les systèmes intelligents sont compréhensibles, traçables et sujettes à un examen minutieux. Le principe de transparence, d'explicabilité et de contestabilité (TEC) fournit une approche structurée : les entreprises doivent concevoir des processus de surveillance et effectuer des « bilans de santé » réguliers pour évaluer dans quelle mesure les systèmes d'IA communiquent clairement leur raisonnement, et dans quelle mesure ils fonctionnent équitablement. En documentant la logique décisionnelle, en divulguant l'utilisation des données et en permettant aux utilisateurs de remettre en question ou de contester les résultats, les entreprises transforment l'IA, la faisant passer d'une boîte noire en un système transparent, responsable et centré sur l'humain, un système dans lequel la visibilité, l'équité et la confiance sont intégrées à chaque décision.

Développement et opérations

Une approche axée sur le respect de la vie privée dès la conception pour le développement et les opérations de l'IA garantit que la protection des données est intégrée à chaque étape du cycle de vie du système, de la conception au déploiement et au-delà. Plutôt que de traiter la confidentialité comme une exigence de conformité ou une question secondaire, elle devient un principe architectural guidant la manière dont les données sont collectées, traitées et conservées. Cela implique de réduire l'utilisation des données au strict nécessaire, d'appliquer l'anonymisation et le cryptage par défaut, et d'intégrer le consentement des utilisateurs et les mécanismes de contrôle

directement dans les flux de travail. La surveillance continue et les évaluations d'impact sur la confidentialité permettent de responsabiliser les systèmes à mesure qu'ils évoluent. En alignant le développement et les opérations sur les principes de confidentialité dès la conception, les entreprises réduisent non seulement les risques réglementaires, mais elles renforcent également la confiance, la résilience et un avantage concurrentiel fondé sur l'innovation éthique.

Réponse aux incidents

Si le chapitre 11 traite de la nécessité d'adopter une approche différente des opérations, il convient de souligner, dans le contexte de la gouvernance de l'IA et de la gestion des risques, que les protocoles de réponse rapide aux défaillances de l'IA, y compris les appels humains et les mesures correctives, sont essentiels à la responsabilisation et à l'amélioration continue.

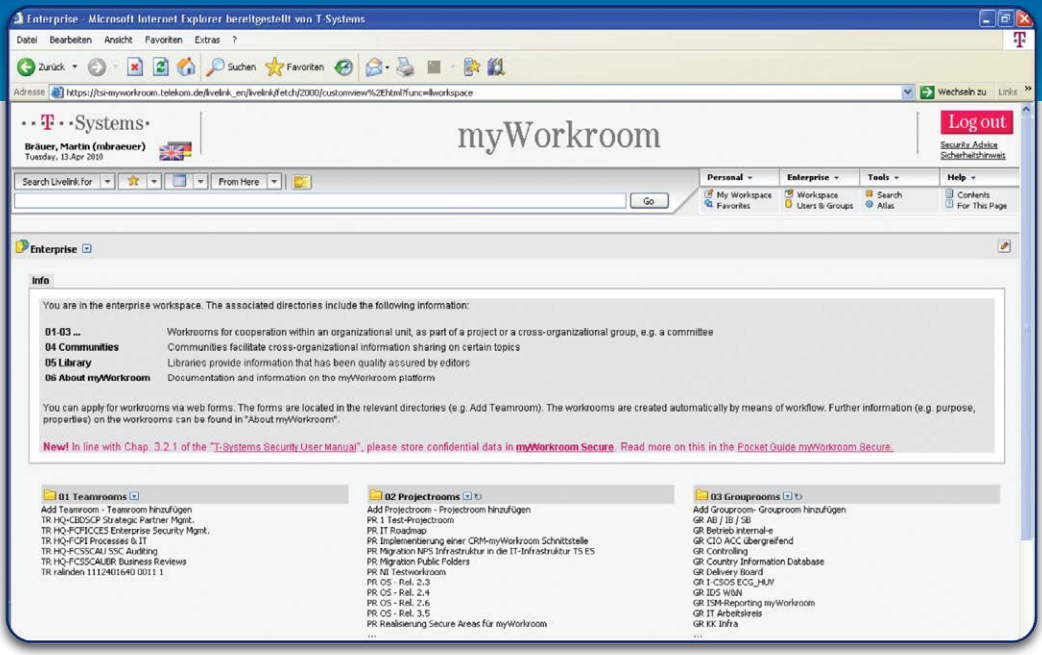
Tous ces éléments sont essentiels pour gérer les risques et préserver la confiance. Étant donné que de nombreuses organisations n'ont pas encore pleinement déployé l'IA, il est utile de réfléchir à l'impact de ces éléments sur votre stratégie globale.

La gouvernance actuelle de l'IA exige également des contrôles de sécurité et de résilience explicites adaptés à l'IA générative. Les cadres de sécurité informatique traditionnels ne couvrent souvent pas les menaces liées aux systèmes génératifs, tels que l'injection rapide, les hallucinations, la manipulation des résultats, etc. Le profil d'IA générative du NIST (projet 2024) et les directives Secure by Design de la CISA (2024) recommandent une modélisation des menaces spécifique à l'IA, une collaboration contradictoire, la surveillance de l'exfiltration des données et le suivi de la provenance des résultats des modèles (CISA, 2024 ; NIST, 2024). Les entreprises devraient mettre en place des mesures pour faire face aux nouveaux risques associés aux modèles génératifs afin de garantir la sécurité, la fiabilité et la responsabilité tout au long du cycle de vie de l'IA générative.

Dans l'article suivant, une entreprise de télécommunications européenne gère le cycle de vie de ses informations pour atteindre ses objectifs de conformité et de gouvernance des données, avec des règles strictes concernant la durée de conservation des informations et le moment où il convient de les éliminer.

Étude de cas

T-Systems



Système de gestion des informations d'entreprise à l'échelle de l'entreprise

Présente dans plus de 20 pays, T-Systems, la marque grand public la plus active de Deutsche Telekom, est le prestataire privilégié de nombreux clients européens majeurs pour leurs activités internationales. Environ 160 000 entreprises et organismes publics utilisent les services intégrés de T-Systems, qu'il s'agisse de gérer des centres de données, des services de protocole Internet mondiaux ou de développer et d'administrer des applications.

Les équipes de T-Systems avaient besoin d'une plateforme leur permettant de se réunir rapidement et facilement pour échanger des informations et garantir l'exécution professionnelle et efficace des projets des clients. Environ 40 000 employés de T-Systems utilisent désormais une plateforme de gestion de contenu d'entreprise (GCE) à l'échelle de l'entreprise pour la collaboration, la gestion des documents et la gestion des connaissances.

T-Systems améliore sa plateforme de collaboration avec une passerelle extranet afin de faciliter la collaboration avec ses clients et partenaires, ainsi qu'un système de gestion du cycle de vie pour les espaces de projet avec des périodes de stockage pouvant aller jusqu'à 10 ans. Cette deuxième fonctionnalité permettra à T-Systems de respecter ses obligations en matière de gouvernance d'entreprise, tout en permettant de rechercher ultérieurement des informations précieuses sur des projets dormants.

Cadres, réglementations et normes de premier plan

Le paysage réglementaire de l'IA évolue rapidement, et la mise en conformité est désormais un moteur de gouvernance majeur. Il existe une combinaison de cadres volontaires, tels que le cadre de gestion des risques (RMF) du National Institute of Standards and Technology (NIST), et de cadres obligatoires (tels que la loi européenne sur l'IA) couverts au chapitre 5. Cependant, les environnements de développement deviennent une exigence pour de nombreuses entreprises pour déployer une approche structurée pour une IA fiable. Les cadres de gouvernance ont pour objectif d'aider à traduire les exigences en contrôles, en politiques et en exigences de supervision afin de guider les entreprises dans leur adoption.

Bien que le paysage réglementaire évolue, il existe aujourd'hui une variété de cadres disponibles qui peuvent aider une entreprise à structurer la gouvernance de l'IA :

Principes de l'OCDE relatifs à l'IA : Adoptés en 2019 par 46 pays et constituant l'une des premières normes en matière de gouvernance de l'IA. Cinq principes clés ont été définis concernant la gouvernance de l'IA, comme suit : [48]

1. L'IA devrait profiter aux personnes et à la planète en favorisant la croissance inclusive et le bien-être.
2. Les systèmes d'IA devraient être conçus pour respecter les droits de l'homme, les valeurs démocratiques et la diversité.
3. Les systèmes d'IA devraient être transparents et explicables.
4. Les systèmes d'IA doivent être robustes, sécurisés et sûrs tout au long de leur cycle de vie.
5. Les entreprises et les individus qui développent, déploient ou exploitent l'IA doivent être responsables de ses résultats.

Loi européenne sur l'IA : Le Règlement du Parlement européen et du Conseil établissant des règles harmonisées sur l'intelligence artificielle (loi sur l'intelligence artificielle) a été adopté en 2024. Il s'agit de l'un des premiers cadres juridiques complets pour l'IA, qui fixe des exigences basées sur différents niveaux de risque, allant du minimum à l'inacceptable. Les principales exigences de la Loi sont les suivantes : [49]

- Transparence pour le contenu généré par l'IA et les systèmes biométriques
- Conformité, tests et documentation stricts pour les systèmes d'IA à haut risque (par exemple, les soins de santé, les infrastructures critiques et l'administration publique)
- Interdiction de l'utilisation de l'IA qui manipule le comportement ou exploite des vulnérabilités
- Supervision humaine obligatoire, systèmes de gestion des risques et alignement sur les réglementations de l'UE en matière de gouvernance numérique et des données

Cadre NIST AI RMF : NIST Risk Management Framework, publié en 2023, est un cadre volontaire et largement adopté pour identifier, évaluer et gérer les risques dans les systèmes d'IA. Il examine la cartographie du contexte et de l'utilisation prévue, la mesure des risques liés à l'IA, la gestion de ces risques par le biais d'une série de contrôles et la gouvernance des systèmes d'IA tout au long de leur cycle de vie. Ce cadre est conçu pour fonctionner parallèlement aux directives de sécurité pour les architectures Zero-Trust.

Le cadre reconnaît que la technologie de l'IA continue d'évoluer : « Le cadre de gestion des risques sur l'IA est conçu pour être pratique, pour s'adapter au paysage de l'IA à mesure que les technologies de l'IA continuent de se développer, et pour être opérationnalisé par les entreprises à des degrés et capacités variés afin que la société puisse bénéficier de l'IA tout en étant protégée contre ses méfaits potentiels. » [50]

ISO/IEC 42001:2023 : L'ISO et la Commission électrotechnique internationale (CEI) ont élaboré des normes pour la gestion et la gouvernance de l'IA. Cela inclut les normes sur les systèmes de gestion de l'IA (AIMS) (ISO/IEC 42001:2023), les concepts et la terminologie de l'IA (ISO/IEC 22989:2022) et les processus du cycle de vie des systèmes d'IA (ISO/IEC 23053:2022).

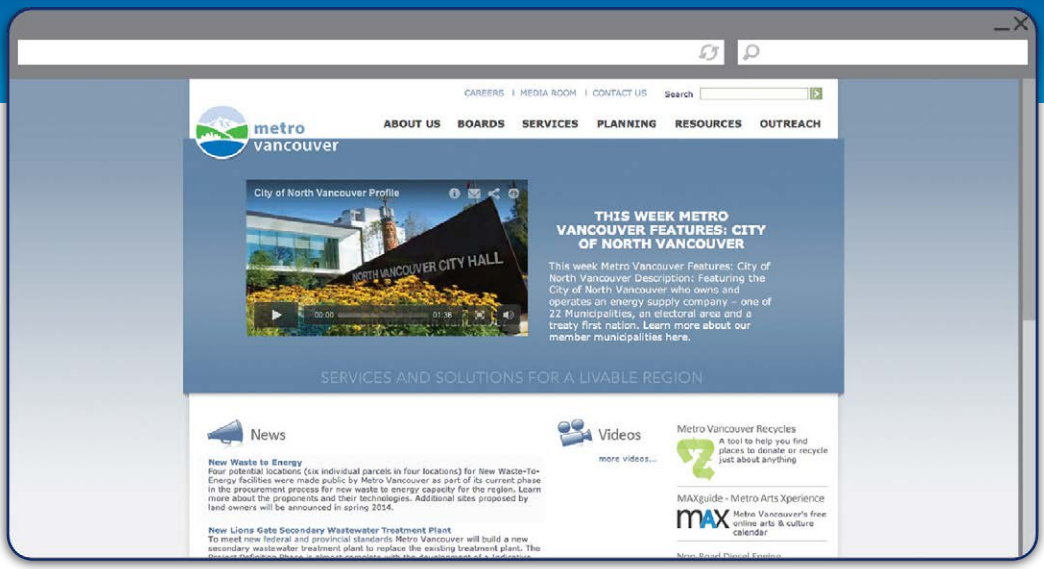
Ensemble, ces normes et principes fournissent aux entreprises une base structurée pour une innovation responsable. Ils traduisent des idéaux de haut niveau (équité, transparence, responsabilité) en pratiques de gouvernance réalisables conformes aux attentes mondiales. En ancrant ses programmes d'IA dans ces environnements de développement, votre entreprise peut créer des systèmes non seulement conformes, mais également cohérents, explicables et fiables au-delà des frontières.

Il existe d'autres normes et cadres, mais ce sont ceux qui sont le plus largement utilisés et adoptés. Au fil du temps, à mesure que la technologie évolue, de nouveaux cadres apparaîtront. Il est donc essentiel d'adopter une approche adaptable de la façon dont vous définissez les contrôles pour éviter de futures retouches.

Dans l'article suivant, la région métropolitaine de Vancouver prouve qu'une bonne gouvernance est une bonne affaire. Une infrastructure essentielle de la GIE contribue à faire en sorte que la Région puisse prouver par le biais d'audits que les documents du système sont des documents fiables et qu'ils sont conformes aux lois et réglementations tout en promouvant les bonnes pratiques commerciales.

Étude de cas

Région métropolitaine de Vancouver



Région métropolitaine de Vancouver

La région métropolitaine de Vancouver est l'un des 29 districts régionaux créés par le gouvernement provincial pour garantir à tous les résidents de la Colombie-Britannique un accès égal aux services dont ils ont généralement besoin. Les parcs régionaux, le logement abordable, les relations de travail et l'urbanisme régional sont des services importants fournis directement au public. La région soutient des milliers d'employés à temps plein et dessert une population de plus de trois millions d'habitants.

La région avait besoin d'un dépôt central et sécurisé pour le stockage et la distribution des dossiers électroniques. Une solution d'administration en ligne leur permettrait d'appliquer des périodes de conservation et des règles d'élimination basées sur des périodes prédéfinies afin de contrôler les risques, de réduire les coûts de stockage et de garantir la conformité réglementaire. La région recherchait également une expérience utilisateur améliorée pour le profilage des documents, notamment en termes d'automatisation et de précision.

Le système contient actuellement près de deux millions de documents. Une solution de gestion automatisée des dossiers élimine les complexités de la gestion des dossiers électroniques, rendant le processus transparent pour l'utilisateur final. Il associe les classifications des enregistrements aux calendriers de conservation, ce qui automatise entièrement le processus visant à garantir que les dossiers sont conservés aussi longtemps que la loi l'exige, puis détruits une fois le temps écoulé. Pour appliquer la gouvernance dans la région, chacun de ses 14 départements est chargé de se conformer aux politiques, aux meilleures pratiques et aux procédures établies par l'équipe chargée des archives de l'entreprise. Le système contribue à faire en sorte que la Région puisse prouver par des audits que les documents du système sont fiables et qu'ils sont conformes aux lois et règlements, tout en promouvant les bonnes pratiques commerciales.

La voie à suivre en matière de gouvernance de l'IAE

La gouvernance de l'IA est essentielle pour les secteurs public et privé. Les délais et la portée de la mise en œuvre sont relativement similaires, mais il existe quelques différences subtiles. Pour le secteur public, l'accent est mis sur la transparence et la confiance des citoyens. La gouvernance repose sur la responsabilité publique, l'éthique et le respect des droits de l'homme. Pour le secteur privé, l'accent est davantage mis sur l'innovation, les risques commerciaux et la conformité réglementaire. La gouvernance est intégrée à la responsabilité sociale des entreprises et aux programmes environnementaux, sociaux et de gouvernance (ESG), afin de trouver un équilibre entre agilité et impact. Les deux secteurs ont intérêt à s'aligner sur les cadres et normes internationales, et ils doivent tous deux considérer la gouvernance de l'IA comme un programme dynamique et évolutif.

Dans l'ensemble, la gouvernance de l'IAE garantit que les principes éthiques, la conformité juridique, la gestion des risques et la responsabilité sont intégrés tout au long du cycle de vie de l'IA et au-delà des frontières organisationnelles. Une gouvernance efficace de l'IA associe des principes de haut niveau à des processus et outils concrets, soutenus par une culture de responsabilité à tous les niveaux. À mesure que les technologies et réglementations relatives à l'IA évoluent, il sera essentiel d'investir en permanence dans la gouvernance, non seulement pour atténuer les risques, mais aussi pour renforcer la confiance, favoriser l'innovation durable et garantir un avantage concurrentiel.

La gouvernance de l'IA va au-delà des considérations purement techniques pour intégrer également les dimensions éthiques et sociales. De nombreuses entreprises adoptent désormais des politiques formelles relatives à l'utilisation responsable de l'IA, intégrant des principes clés tels que l'équité, la transparence, la responsabilité et le respect des droits de l'homme tout au long du cycle de vie de l'IA. Ces garde-fous deviennent essentiels, non seulement pour garantir la conformité, mais aussi pour maintenir la confiance dans les opérations pilotées par l'IA. Sans eux, les promesses des systèmes intelligents risquent d'être minées par des manquements à l'éthique, des atteintes à la vie privée ou des défaillances de gouvernance.

La prochaine vague de gouvernance de l'IA concerne l'alignement et le contrôle de systèmes d'IA autonomes et agentiques capables de lancer des actions sans approbation humaine explicite. Les exigences de gouvernance s'étendent pour inclure les limites d'autonomie, la supervision en temps réel et les voies d'escalade lorsque les modèles affichent des comportements trompeurs ou axés sur des objectifs (UK AI Safety Institute, 2024). De même, les seuils de calcul et de capacité deviennent un outil politique permettant de déterminer quand le développement de l'IA doit déclencher un examen externe (NIST, 2024 ; CISA, 2024). Pour les entreprises, cela signifie que la gouvernance de l'IAE doit passer d'une conformité statique aux politiques à une surveillance continue, à une assurance et à une gestion adaptative des risques. Les entreprises qui institutionnalisent la gouvernance de l'IA en tant que système vivant de contrôle, de supervision et de validation externe seront les mieux placées pour innover de manière responsable à l'avant-garde.

Dans l'étude de cas suivante, découvrez comment un leader des logiciels d'entreprise a réduit le nombre de types de documents de 96 % pour se préparer à l'innovation et à l'automatisation en matière d'intelligence artificielle.

Étude de cas

Un fournisseur mondial de PRE

> *Les possibilités de libre-service pour les employés sont illimitées. Par exemple, si un employé soumet un document pour modifier son adresse ou son état civil, l'automatisation IA peut mettre à jour son dossier professionnel sans qu'aucun membre de l'équipe des ressources humaines n'intervienne.*
>
> Responsable de la prestation mondiale des ressources humaines

La gestion de millions de dossiers d'employés au sein d'un effectif mondial présentait d'importants défis en matière de gouvernance et de conformité. Les processus manuels et fastidieux rendaient les exigences réglementaires, comme le RGPD, difficiles à respecter de manière cohérente, tandis que les systèmes vieillissants n'étaient pas compatibles avec les technologies RH de nouvelle génération. Pour soutenir la modernisation, l'entreprise a décidé de transformer son cadre de gouvernance des informations, en automatisant la conformité et en intégrant « la sécurité et la confidentialité dès la conception » à chaque étape de la gestion des données RH.

Le nouveau modèle de gouvernance a unifié les politiques de conservation, de destruction et d'accès aux documents dans toutes les régions, en remplaçant des milliers de modèles incohérents par des formats mondiaux standardisés. La planification automatisée de la rétention et les politiques de suppression garantissent désormais une conformité continue, réduisant ainsi les risques opérationnels tout en libérant les équipes RH de toute supervision manuelle. Un chiffrement renforcé des contrôles d'accès et des pistes d'audit consolide l'intégrité des données, tandis que l'automatisation de la gouvernance permet une prise de décision plus rapide et plus fiable.

Cette base étant en place, l'entreprise se prépare à passer à la phase suivante, qui consiste à tirer parti de l'IA pour améliorer la classification des documents, automatiser la gestion des dossiers et renforcer la gouvernance à grande échelle. En combinant des contrôles techniques robustes avec de solides mécanismes de supervision et de responsabilisation, elle passe du maintien de la conformité à une gouvernance proactive, créant ainsi un environnement sécurisé, piloté par les données, prêt à l'innovation intelligente.

Télécharger The Fast Five

1. **Faites de la gouvernance de l'IA un impératif stratégique.**
   Mettez en place un soutien exécutif et une prise en charge claire de la gouvernance de l'IA afin de garantir que toutes les initiatives sont conformes aux objectifs éthiques, juridiques et organisationnels.

2. **Intégrez l'éthique et la responsabilité dans le cycle de vie de l'IA.**
   Intégrez des directives éthiques, des contrôles des risques, des mesures de conformité réglementaire et de responsabilisation à chaque étape, de la conception au déploiement et à la surveillance, afin de prévenir activement les biais et les préjudices involontaires.

3. **Activez les principaux cadres et normes.**
   Mettez en œuvre des environnements de développement tels que les principes de l'OCDE, la loi européenne sur l'IA, le NIST AI RMF et la norme ISO 42001 pour traduire les meilleures pratiques et les exigences réglementaires en contrôles et en supervision réalisables.

4. **Intégrez la gouvernance de l'IA dans l'ensemble de l'entreprise.**
   Alignez la gouvernance de l'IA avec la gouvernance de l'entreprise, de l'informatique et des données en clarifiant les rôles, les responsabilités et les processus, en garantissant une supervision complète depuis la planification du projet jusqu'à la mise hors service.

5. **Favorisez l'amélioration continue et la confiance.**
   Instituez des audits permanents, adaptez les protocoles de gouvernance à mesure que les technologies et les réglementations évoluent, et intégrez une culture d'apprentissage et de responsabilité afin de maintenir la confiance et la valeur à long terme.

Chapitre sept

L'architecture des déploiements de l'IAE souveraine

Comme décrit dans les chapitres précédents, 90 % des données du monde sont bloquées derrière des pare-feu et résident dans des environnements privés, propriétaires ou sensibles. Dix pour cent seulement sont accessibles au public, et c'est cette minorité qui a largement contribué à la première vague d'IA générative. Pour exploiter tout le potentiel de l'IA générative, de l'IA agentique et, en fin de compte, de l'intelligence artificielle générale (IAG), les entreprises des secteurs public et privé doivent développer des mécanismes sécurisés et souverains pour accéder aux 90 % et les utiliser sans compromettre la confidentialité, la sécurité ou le contrôle national. Dans ce chapitre, nous allons vous montrer comment vous pouvez le faire en utilisant une approche hybride qui intègre les données souveraines et l'IAE sur une plateforme GIE.

> *Les nouveaux risques, tels que le fait que les administrations étrangères soient habilitées à appuyer sur le kill switch (interrupteur d'arrêt d'urgence), ont suscité des inquiétudes au sein des entreprises internationales.* [51]

Dans l'économie numérique d'aujourd'hui, les données constituent l'actif le plus fondamental. Elles sont l'engrais de l'innovation, stimulent la productivité et soutiennent la sécurité nationale. Alors que l'IA transforme tous les secteurs et que les considérations géopolitiques évoluent rapidement, il est plus important que jamais pour les dirigeants de garantir la confidentialité et la protection de leurs données, de leurs infrastructures et de leurs capacités IA. Ce défi s'étend de l'entreprise au niveau national, où il est impératif que les pays élaborent des plans souverains pour le leadership en matière d'IA.

La capacité d'un pays à être à l'avant-garde de l'ère de l'IA dépend de sa capacité à contrôler et à exploiter sa ressource numérique la plus précieuse : les données. Sans un contrôle absolu, les pays risquent de voir leur infrastructure numérique annexée – soit techniquement, soit juridiquement – par des juridictions étrangères. Il ne s'agit pas simplement d'une question d'innovation ; c'est une question de sécurité nationale.

Les responsables informatiques considèrent de plus en plus la souveraineté de l'infrastructure et des données comme un impératif stratégique. Dans un monde marqué par les tensions géopolitiques, les restrictions commerciales et l'évolution rapide des cadres réglementaires, la dépendance à l'égard de fournisseurs éloignés ou soumis à des contraintes politiques est devenue un risque commercial important. Les entreprises visionnaires ne se contentent pas de respecter leurs obligations en matière de conformité ; elles adoptent des architectures résilientes et adaptées à leur juridiction, capables de résister aux perturbations, de garantir la sécurité juridique et d'assurer la continuité des opérations en toutes circonstances. [52]

Définitions de la souveraineté numérique

Les discussions mondiales sur les données et l'IA se concentrent de plus en plus sur l'importance de la souveraineté numérique. Cela fait référence à la capacité d'un pays ou d'une entreprise à garder le contrôle de ses actifs numériques, de ses données, de ses systèmes et de ses opérations, en garantissant son indépendance vis-à-vis des influences extérieures et le respect des réglementations nationales.

En fonction de la sensibilité des données, la réalisation de la souveraineté numérique peut nécessiter un ou plusieurs des éléments suivants :

- **Souveraineté des données** : garantir que les données sont stockées, traitées et gérées au sein d'une juridiction spécifique, avec des contrôles stricts pour empêcher l'accès ou le transfert à des entités étrangères ou en vertu de lois étrangères.
- **Souveraineté opérationnelle** : s'assurer que les opérations sont situées dans une juridiction spécifique et que le personnel chargé de la gestion des actifs numériques sont des citoyens de cette juridiction et possède les autorisations de sécurité appropriées.
- **Souveraineté technologique** : conserver le contrôle de l'infrastructure, notamment de la sécurité physique des centres de données, des droits d'accès et de la gestion du matériel, des logiciels et des clés de chiffrement. Cela inclut la souveraineté du plan de contrôle, un ensemble de services essentiels à l'intégration des applications avec l'infrastructure sous-jacente.
- **Souveraineté juridique** : s'assurer que les fournisseurs de technologies et les fournisseurs de services cloud sont régis exclusivement par le droit d'une juridiction spécifique.

Une approche hybride équilibrée

Pour être compétitifs à l'ère de l'IA, les pays doivent tirer parti de l'ampleur, de l'innovation et de la flexibilité des services de cloud public mondiaux. Cette nécessité crée toutefois une tension fondamentale avec l'impératif sécuritaire qui consiste à maintenir le contrôle souverain. Un modèle hybride est la solution essentielle pour relever ce défi. Cette approche équilibre les deux exigences en reconnaissant que toutes les données ne nécessitent pas le même niveau de protection. Les données souveraines sensibles sont protégées sur des plateformes sécurisées et une couche d'infrastructure détenue et exploitée au niveau national, tandis que les ensembles de données publics et les services destinés aux citoyens peuvent utiliser des hyperscalers mondiaux pour atteindre la charge nécessaire.

Découvrez comment un leader mondial des technologies et des services a tiré parti d'une approche hybride des données et de l'IA générative pour analyser des cas historiques impliquant des millions de documents et des milliers de téraoctets.

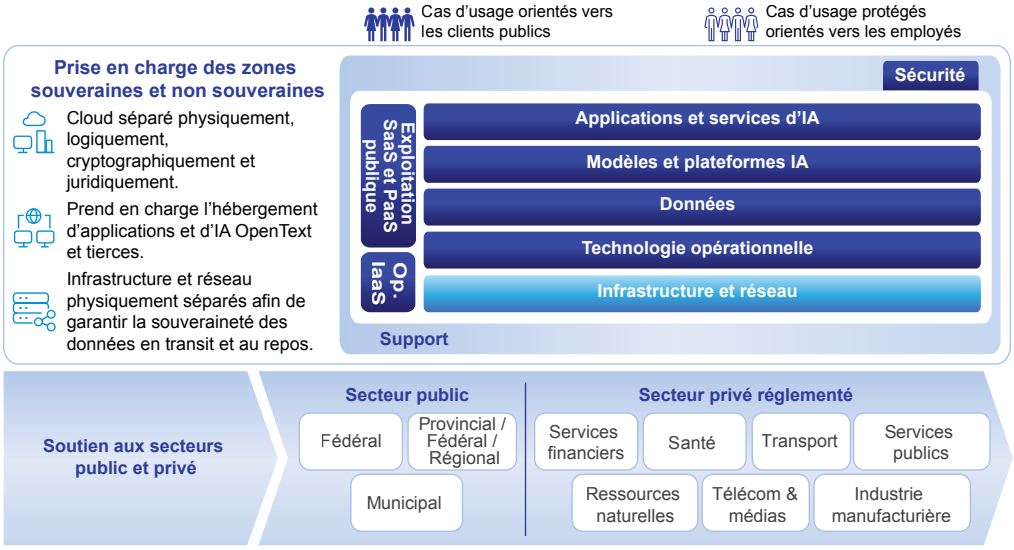
Étude de cas

Un leader technologique mondial

Ce leader mondial de la technologie et des services façonne les tendances universelles en matière d'automatisation, d'électrification, de numérisation et de connectivité. Sa forte présence industrielle stimule l'innovation pour améliorer les processus, notamment en optimisant les opérations juridiques.

En tant qu'entreprise internationale, les défis juridiques sont inévitables lorsqu'on opère à grande échelle, mais les longues enquêtes internes et les évaluations préliminaires fastidieuses entravaient leur capacité à définir les prochaines étapes et empêchaient l'entreprise d'innover et de créer de la valeur. L'inefficacité des processus a entraîné une augmentation des coûts et des risques, en raison de l'absence de technologie permettant de soutenir la connaissance des dossiers et le contrôle dès le début du processus. L'entreprise recherchait une solution technologique pour l'aider à prendre des décisions plus éclairées et plus rapides en traitant et en analysant rapidement de grandes quantités de données internes, et pour contribuer à définir la manière dont l'affaire judiciaire allait se dérouler.

L'entreprise a adopté une approche hybride. Leur équipe juridique l'a utilisée avec une IA générative pour analyser de vastes ensembles de données lors de la phase d'évaluation des dossiers. Ils ont ensuite utilisé un vaste modèle linguistique pour poser les questions pertinentes et obtenir des réponses en quelques minutes afin de déterminer leur stratégie de cas. L'entreprise internationale a pu transformer ses flux de traitement juridiques, permettant des décisions plus rapides basées sur les données et des enquêtes proactives. Grâce à l'intégration de l'IA et à la formation, ses équipes juridiques ont été en mesure de fournir un service supérieur.



Architecture de haut niveau des données souveraines et de l'IA

L'architecture pour la souveraineté

Le cadre architectural ci-dessus fournit une vue d'ensemble des composants essentiels pour Le cadre architectural ci-dessus offre une vue d'ensemble des composants essentiels permettant de mettre en œuvre les capacités de données souveraines et d'IA sur une plateforme GIE pour les secteurs public et privé. Ce cadre garantit que des services sécurisés sont fournis aux clients de manière efficace, en protégeant leurs données critiques.

Les principaux aspects de cette architecture sont les suivants :

- **Double architecture de données** : les données sensibles sont protégées au cœur d'une couche souveraine, tandis que les données accessibles au public sont traitées dans un environnement cloud hybride (c'est-à-dire un environnement qui intègre le cloud public et privé).
- **Modèle IA multiagents** : les « agents d'IA privés » opèrent au sein de la sphère souveraine, tandis que les « agents d'IA publics » fournissent des services via le cloud hybride, garantissant ainsi la sécurité des frontières et l'intégrité des données.
- **Extensibilité** : Conçu pour intégrer des ensembles de données supplémentaires.
- **Sécurité et gouvernance des données** : respect des politiques et des contrôles relatifs à la protection et à l'utilisation des données.
- **Principes fondamentaux** : confiance, sécurité, contrôle national et résilience.

Ce qui suit est un aperçu de l'architecture ci-dessus.

La couche infrastructure et réseau

Les données sensibles sont hébergées dans une infrastructure gérée par des fournisseurs de télécommunications et de centres de données fiables. Ces environnements sont conçus pour répondre aux exigences de sécurité et de souveraineté les plus strictes, en utilisant des protocoles Zero-Trust – des cadres de sécurité qui vérifient chaque connexion, chaque appareil et chaque utilisateur en permanence plutôt que de supposer qu'un élément est sûr – et des configurations isolées, dans lesquelles les systèmes critiques sont physiquement ou logiquement isolés des réseaux publics afin d'empêcher tout accès non autorisé ou toute fuite de données. Les déploiements se font à l'intérieur des frontières nationales ou régionales définies, les opérations étant gérées exclusivement par du personnel habilité en matière de sécurité afin de garantir le respect de toutes les lois, réglementations et normes de défense applicables.

Pour les données et les charges de travail qui ne nécessitent pas une souveraineté totale, telles que les ensembles de données accessibles au public ou les expériences numériques destinées aux citoyens et aux clients, le cadre intègre des hyperscalers mondiaux. Ces plateformes fournissent la taille, la flexibilité et les outils avancés requis pour soutenir l'innovation, la réactivité et la rentabilité, tout en fonctionnant dans des limites de gouvernance strictes qui les empêchent de rentrer en contact avec les données souveraines.

Dans les deux zones, l'architecture est unifiée par un ensemble technologique commun intégrant des fonctionnalités dans les domaines de la gestion des données et des informations, des modèles d'IA et des applications d'IA.

La couche technologique opérationnelle

La couche technologique opérationnelle est essentielle pour permettre le déploiement de données, de modèles d'IA, de plateformes, d'applications et de services d'IA. Elle fait le pont entre l'infrastructure, le réseau et les applications.

Dans un monde multicloud et hybride, la standardisation au niveau de la couche opérationnelle est essentielle. L'adoption de protocoles ouverts et de cadres interopérables permet aux entreprises de maintenir la portabilité des charges de travail, c'est-à-dire la capacité de déplacer des applications et des données de manière transparente entre des clouds sur site, privés et souverains sans refactorisation ni compromis en matière de sécurité. Ceci est particulièrement important pour les charges de travail d'IA, où l'intensité de calcul, la gravité des données et les contraintes réglementaires exigent à la fois flexibilité et contrôle.

La gouvernance des technologies opérationnelles s'étend également à la surveillance, à l'observabilité et à l'automatisation. Des plans de contrôle et des outils d'orchestration unifiés garantissent des configurations cohérentes, une gestion des correctifs et une vérification de conformité en temps réel. En ce sens, la couche opérationnelle garantit que chaque déploiement d'IA, de la formation des modèles à l'inférence, s'effectue dans des limites fiables, adhère à des juridictions définies et évolue en toute confiance.

La couche de données

En tant que base de l'IAE, la couche de données doit répondre aux besoins des secteurs public et privé. Elle permet une gestion des données sécurisée, intelligente et évolutive dans les secteurs public et gouvernemental, avec l'extensibilité nécessaire pour répondre aux besoins du secteur privé.

L'architecture nécessite la prise en charge des hiérarchies de données explicites et implicites. Les structures explicites incluent les hiérarchies de dossiers, les taxonomies, les schémas, le contrôle de version et les journaux d'audit. Les structures implicites incluent les champs de métadonnées, les relations sémantiques, les ontologies, les balises et le regroupement basé sur l'utilisation. Elles sont combinées à l'aide d'une orchestration basée sur les métadonnées et de moteurs sémantiques, permettant aux systèmes d'IA de raisonner à la fois sur des données structurées et non structurées.

Cas d'utilisation agentique

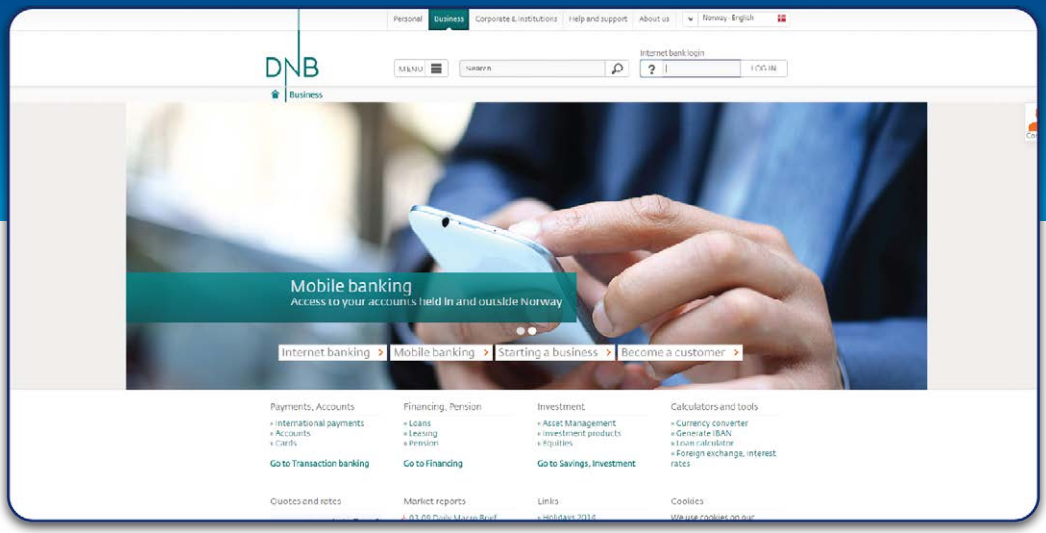
Les agents stimuleront la productivité et l'efficacité tout en offrant un meilleur service à la clientèle et de meilleurs résultats commerciaux. Voici quelques exemples d'utilisation de l'IA agentique :

- **Soins de santé** : navigation personnalisée en matière de santé, éligibilité aux prestations et triage virtuel
- **Logement** : traitement des demandes, délivrance des permis, vérification de l'éligibilité et gestion des subventions
- **Services bancaires** : détection proactive des fraudes, conseils financiers personnalisés et traitement automatisé des prêts
- **Transport** : optimisation dynamique des itinéraires, gestion de flotte autonome et maintenance prédictive
- **Fiscalité** : signalement des audits, détection des fraudes et assistance pour remplir les déclarations fiscales

Dans l'étude de cas suivante, découvrez comment DNB Finans utilise l'IA et les données pour rationaliser l'administration des flottes automobiles, détecter les fraudes et améliorer la satisfaction de ses clients loués.

Étude de cas

DNB Finans



DNB Finans

Le groupe DNB Bank en Norvège est la deuxième plus grande banque de Scandinavie, employant 13 430 personnes et gérant un actif total de 250 milliards d'euros (273 milliards de dollars américains). Sa filiale, DNB Finans, est l'une des plus grandes sociétés de financement des pays nordiques. Dans le secteur privé, l'entreprise occupe une position dominante sur le marché du financement automobile avec plus de 300 000 véhicules financés dans son portefeuille.

DNB Finans est toujours à la recherche de nouvelles façons d'apporter de la valeur ajoutée à ses clients. Les services les plus appréciés proposés sont ceux qui aident les entreprises à contrôler leurs coûts en leur offrant une meilleure visibilité sur leurs dépenses. À cette fin, la division Autolease de DNB Finans souhaitait approfondir la BI qu'elle fournissait à ses clients. Par exemple, le système pourrait fournir des statistiques à jour pour aider les clients à suivre tous les coûts liés à la voiture, y compris des informations sur la consommation de carburant, les émissions de CO^2, les coûts de location, les rapports de dommages et les alertes de fraude. Dans le même temps, la société devait établir des structures de centres de coûts personnalisées afin que les clients puissent suivre l'activité par unité commerciale. DNB Finans tenait à ce que le logiciel soit facile à utiliser sans formation. L'objectif était de proposer une expérience utilisateur similaire à celle des réseaux sociaux grand public tels que Facebook.

La société a déployé une solution d'intelligence commerciale et de création de rapports destinée à être utilisée par plus de 30 000 clients de voitures louées. La solution est très intuitive, avec des représentations visuelles colorées des données, notamment des tableaux de bord pour les utilisateurs et des contrôles logiques pour la détection des fraudes et l'administration simplifiée des flottes automobiles. Depuis le déploiement, DNB Finans a vu le niveau de satisfaction de ses clients passer de 4,4 à 5,1 sur une échelle de 1 à 6 pour la « qualité de la solution de création de rapports ».

Le système a également attiré 31 % de connexions d'utilisateurs supplémentaires, augmentant ainsi l'activité du système de financement automobile. DNB Finans prévoit un retour sur investissement d'ici deux ans et demi. Ses clients ont désormais une visibilité précoce sur des problèmes tels que le kilométrage excessif ou les fraudes liées au carburant, et sont en mesure d'identifier les unités commerciales responsables, d'améliorer leur capacité d'action et de fidéliser leurs clients grâce à des informations commerciales précieuses. Cette solution confère à l'entreprise un avantage concurrentiel significatif sur un marché très concurrentiel.

Architecture détaillée des données souveraines et de l'IA

Double architecture de données

Le schéma ci-dessus présente une architecture détaillée pour une plateforme de données et d'intelligence artificielle sécurisée à deux zones, en distinguant les environnements de la zone non souveraine ou publique et de la zone souveraine ou privée.

L'objectif de cette architecture est de garantir que les données et activités sensibles des entreprises et du gouvernement sont séparées des domaines publics ou moins sensibles, tout en permettant des interactions contrôlées si nécessaire dans le domaine public. Elle répond aux besoins en matière de sécurité des données et d'intelligence artificielle, tout en offrant la flexibilité nécessaire à l'efficacité et à la rentabilité des déploiements, permettant ainsi d'améliorer l'expérience client.

Analysons cela plus en détail.

La zone publique et non souveraine

Dans une architecture de données et d'IA à double souveraineté, la zone publique sert d'interface contrôlée entre le savoir à accès libre et l'intelligence d'entreprise. Elle permet aux entreprises de tirer parti de données non sensibles accessibles au public et de services d'intelligence artificielle sans compromettre la souveraineté interne ni les obligations de conformité. En isolant les interactions publiques grâce à des passerelles sécurisées et à des protocoles de désinfection, la zone publique permet à l'innovation et à la connectivité externe de prospérer dans des limites clairement définies et gouvernées.

Cette zone est composée de :

Agents d'IA publics et non sensibles : Cette fonctionnalité comprend des interfaces telles que les API de modèles linguistiques à grande échelle (MLE) qui n'utilisent pas de données sensibles. La couche API des agents publics fournit des points de terminaison pour accéder aux données, avec des mesures pour contrôler l'utilisation, sécuriser les sessions et stocker les données de session.

Sources de données publiques ou non souveraines : Ici, le système accède à des bases de données publiques et non sensibles, à des réglementations publiées et à des guides de service. Il utilise également des bases de connaissances publiques afin d'améliorer la précision et la pertinence des informations qu'il fournit.

Contrôles de sécurité : les mesures de sécurité incluent le nettoyage des informations personnelles identifiables (IPI) à l'aide de modèles de reconnaissance d'entités nommées (REN) pour supprimer les informations sensibles telles que la date de naissance avant toute validation par passerelle.

La zone souveraine / privée

La zone souveraine ou privée est le cœur du renseignement d'une architecture de données et d'intelligence artificielle à double souveraineté, dans laquelle les activités sensibles et critiques se déroulent sous le contrôle total de l'entreprise. Conçue pour les environnements réglementés et hautement sécurisés, cette zone régit l'utilisation d'agents privés, de sources de données confidentielles et d'une infrastructure informatique sécurisée. Chaque processus, de la formation du modèle à l'inférence, est exécuté dans un cadre Eero-trust et isolé, garantissant que les données nationales, d'entreprise ou institutionnelles restent totalement souveraines, conformes et contrôlables.

Cette zone est composée des éléments suivants :

Agents privés : Cette fonctionnalité est réservée aux utilisateurs des entreprises du secteur public ou du secteur privé et aux agents qui accèdent à des données sensibles. Elle contient une plateforme agentique capable de se déployer dans des espaces isolés. La couche d'API d'agent privé est ici uniquement interne, avec une sécurité Zero-Trust.

Sources de données souveraines : Cela inclut les bases de données protégées contenant des informations sensibles, notamment des données relatives aux ressources humaines ou aux finances, ainsi que des dossiers ministériels sensibles. Dans ce contexte, le pipeline de génération augmentée par la recherche (GAR) utilise des sources de connaissances protégées, notamment des précédents juridiques, pour produire des résultats d'IA précis.

La GAR est essentielle dans l'IA d'entreprise, car elle donne aux modèles un accès aux connaissances pertinentes au moment de l'exécution, au lieu de se fier uniquement à ce sur quoi ils ont été formés. Les premières implémentations, souvent appelées « GAR naïves », se contentaient de récupérer des morceaux de texte et de les insérer dans des prompts, ce qui pouvait être imprécis et susceptible d'entraîner des hallucinations lorsque le contexte n'était pas parfaitement aligné. La GAR basée sur des graphes (Graph-GAR) représente la prochaine évolution : elle structure les connaissances de l'entreprise sous forme de relations et d'entités, permettant au modèle de récupérer non seulement des documents, mais aussi leur signification contextuelle appropriée. En conséquence, Graph-GAR améliore considérablement la précision, la traçabilité et la confiance, réduisant ainsi le besoin de messages trop volumineux et de « remplissage de contexte » peu fiable.

Aujourd'hui, les entreprises disposent de trois méthodes principales pour fournir du contexte aux modèles d'IA : des instructions volumineuses et bien conçues dans des fenêtres contextuelles étendues, des flux de récupération GAR/Graph-GAR et le réglage du modèle (y compris le réglage fin et l'intégration de l'optimisation). L'avenir de l'IA d'entreprise réside dans l'orchestration intelligente de ces éléments, en passant d'une ingénierie manuelle de prompts à des flux contextuels régis, structurés et évolutifs qui permettent aux systèmes d'IA de raisonner à partir des connaissances de l'entreprise de manière sécurisée et fiable.

Infrastructure de traitement : fournit une capacité de calcul accélérée pour des charges de travail sécurisées. Cela inclut une base de données de pistes d'audit immuable pour le contrôle de la conformité et le réglage fin optionnel des MLE.

Composants partagés et mesures de sécurité

Entre ces zones se trouve une passerelle API qui applique des protocoles d'authentification/autorisation stricts, notamment la vérification d'identité via la fédération de contrôle d'accès et l'authentification multifactorielle (MFA). Les mécanismes de classification des données balisent automatiquement le contenu par niveau de sensibilité. Les outils de prévention des pertes de données bloquent les fuites de données sensibles au-delà des frontières.

Un routeur de requêtes dirige les demandes vers la zone appropriée en fonction du niveau de classification. Seules les réponses déclassifiées pour le public sont autorisées à revenir dans le domaine non souverain après la suppression des données protégées.

La couche infrastructure et réseau

Les deux zones tirent parti d'une infrastructure et de couches réseau robustes, garantissant une séparation physique et/ou logique lorsque cela est nécessaire.

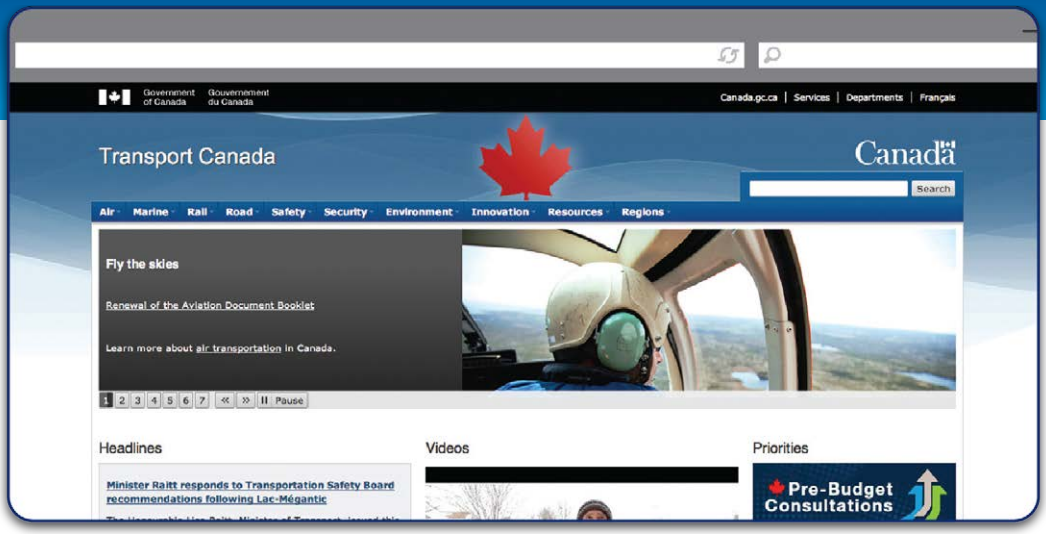
Les données souveraines ne sont pas un « nouveau » concept : historique des cas d'utilisation dans le secteur privé

Les cas d'utilisation du secteur privé dans des secteurs réglementés et non réglementés peuvent aider à encadrer et à façonner cette architecture souveraine. La protection des données privées et sensibles est une nécessité depuis des décennies, et une solide gestion des informations est essentielle pour y parvenir.

L'article suivant sur Transports Canada démontre comment une gestion efficace de l'information permet de mettre à la disposition des utilisateurs des contenus sécurisés et d'intégrer les contenus essentiels aux processus opérationnels.

Étude de cas

Transports Canada



Transports Canada

La mission de Transports Canada consiste à servir l'intérêt public en promouvant un système de transport sûr, sécuritaire, efficace et respectueux de l'environnement au Canada. Cela nécessite une gestion efficace de l'information afin de faciliter la prise de décisions éclairées en temps opportun parmi un large éventail de partenaires du portefeuille, qui comprend 15 sociétés d'État, 17 administrations portuaires et 21 administrations aéroportuaires, ainsi que d'autres organismes à gouvernance partagée.

Soucieux de la diffusion de l'information par voie électronique, de la protection de la vie privée, de la perte de mémoire d'entreprise due au roulement du personnel et de la nécessité d'accéder en temps réel à l'information pour répondre aux demandes et aux préoccupations liées aux litiges, le gouvernement du Canada (GC) a promu une solution d'administration électronique fondée sur la gestion des dossiers, des documents et de l'information. Transports Canada a été le premier ministère fédéral canadien à mettre en œuvre un projet d'administration électronique, avec plus de quatre millions de documents dans une seule bibliothèque et 5 200 utilisateurs sur plus de 117 sites, ce qui en fait le plus grand déploiement de bibliothèque dans le secteur public canadien.

Fonctionnant comme un ensemble intégré d'outils qui facilite l'utilisation complète de la documentation électronique – de la saisie et du stockage à l'organisation, la récupération, le partage, la réutilisation, la protection et la suppression des informations –, cette solution est devenue une application essentielle pour les gestionnaires et le personnel de Transports Canada. Cela a permis à l'entreprise de garantir l'exactitude de ses registres d'entreprise, de rassembler une main-d'œuvre dispersée géographiquement et mobile, de respecter ses obligations légales, y compris les exigences en matière de découverte électronique, d'améliorer sa productivité et d'aligner la gestion de l'information sur l'initiative Gouvernement en ligne (GOL). Grâce à ce système, Transports Canada a triplé ses économies de productivité, économisant jusqu'à 4,6 millions de dollars, et prévoit une croissance supplémentaire, tout en restant en bonne voie pour atteindre son objectif annuel de réduction des coûts. En conséquence, le système a été rentabilisé en 1,17 an seulement.

L'adoption du cloud ayant augmenté ces dernières années, la plupart des entreprises utilisent un modèle hybride de déploiement sur site, dans des centres de données et dans des environnements de cloud public. À mesure que l'adoption de l'IA augmente, il est tout à fait naturel que ces modèles de déploiement éprouvés évoluent pour prendre en charge un modèle hybride pour l'IA.

Le Bundesrechenzentrum (BRZ) en Autriche a opté pour une approche hybride, en s'appuyant sur un système de gestion de l'information basé sur le cloud pour consolider et gérer les données sensibles de 12 clients gouvernementaux, 40 applications gouvernementales, plus de 10 systèmes PRE et des systèmes de messagerie.

Étude de cas

Bundesrechenzentrum (BRZ)

Gestion de l'information basée dans le cloud chez BRZ

Le Centre fédéral de calcul (Bundesrechenzentrum, ou BRZ) est le prestataire de services informatiques de l'administration publique autrichienne. Avec 1 200 employés et un chiffre d'affaires annuel total de 265,3 millions d'euros, le BRZ développe et fournit efficacement des services administratifs en ligne pour les ministères, les universités, les organismes de sécurité sociale et les organisations publiques. Le BRZ exploite 320 processus informatiques, équipe 1 200 sites en Autriche en infrastructures et dessert environ 30 000 postes de travail.

En 2000, les registres fonciers et commerciaux du ministère autrichien de la Justice étaient un exemple typique de fragmentation des processus. Alors que les données du registre foncier étaient gérées numériquement depuis les années 1980, les documents originaux restaient dans les archives physiques des palais de justice et étaient inaccessibles dans le cadre des processus. De plus, le ministère de la Justice a dû faire face à des coûts élevés liés à la conservation des archives et au risque de perte des documents originaux.

Le BRZ a décidé de résoudre le problème en mettant en œuvre une solution de gestion de contenu d'entreprise (GCE). Au fur et à mesure de la mise en œuvre de l'étude pilote pour le cadastre, le BRZ a reçu davantage de demandes de la part des administrations pour gérer les documents par voie électronique et intégrer les processus. En réponse, le BRZ a construit une infrastructure GCE évolutive appelée « eGov Archive Service », le tout premier service GCE-cloud privé autrichien.

La solution a fourni une plateforme robuste pour 12 clients gouvernementaux, 40 applications gouvernementales, plus de 10 systèmes PRE et systèmes de courrier. Le service d'archivage eGov gère 45 téraoctets (To) de données ou 400 millions d'objets, traite environ 1 million de transactions par jour et est consulté par 30 000 utilisateurs (auditeurs fiscaux, juges, policiers, douaniers, personnel des ressources humaines et comptables) et potentiellement par tous les citoyens autrichiens. Les services proposés englobent la gestion, l'accès, le routage et la recherche, ainsi que l'archivage conforme à la législation de tous types de documents. Ils comprennent également une intégration étroite avec les systèmes métier et les progiciels de gestion intégrée (PRE) pour offrir une solution cloud complète.

Fondation pour l'IA agentique

Débloquer les données privées du monde entier est le principal défi de la prochaine vague d'intelligence artificielle. Ce chapitre fournit le plan architectural permettant de le faire en toute sécurité. La solution est un modèle hybride à deux zones qui établit une zone privée sécurisée pour les actifs sensibles et une zone publique pour les autres charges de travail. Ce modèle crée un environnement sécurisé dans lequel les agents d'IA privés peuvent analyser et agir sur les données protégées des entreprises ou des administrations sans risque de fuite, tandis que les agents d'IA publics s'occupent de tâches non souveraines, en équilibrant le contrôle avec l'échelle et la compétitivité. Cette architecture constitue le fondement essentiel à l'activation de l'IA avancée, en apportant la confiance et le contrôle nécessaires au déploiement à grande échelle de l'IA agentique, sujet que nous aborderons dans le chapitre suivant.

Télécharger The Fast Five

1. **Mandatez un contrôle souverain des données.**
   Priorisez et exercez un contrôle total sur les données nationales et d'entreprise et sur l'infrastructure numérique. Établissez des politiques et des mesures techniques pour empêcher toute influence extérieure, garantir la résidence des données et assurer le respect des réglementations nationales.

2. **Mettez en œuvre une architecture d'IA hybride à deux zones.**
   Séparez les données sensibles et les charges de travail dans une infrastructure sécurisée gérée au niveau national. Tirez parti des plateformes de cloud public uniquement pour les applications évolutives et non sensibles afin de trouver un équilibre entre innovation et sécurité.

3. **Déployez des modèles d'IA multiagents de manière stratégique.**
   Activez des agents d'intelligence artificielle privés dans les zones protégées pour analyser les données sensibles et agir sur celles-ci. Utilisez des agents d'IA publics pour des tâches non souveraines, permettant aux entreprises de développer l'innovation en matière d'IA sans compromettre les actifs protégés.

4. **Appliquez une gouvernance et une sécurité rigoureuses.**
   Appliquez une authentification stricte, une classification avancée des données et des outils robustes de prévention des pertes de données. Assurez-vous que toutes les activités critiques sont enregistrées à l'aide de pistes d'audit immuables et qu'elles fonctionnent selon des protocoles de confiance zéro pour une surveillance et une résilience maximales.

5. **Accélérez l'adoption d'architectures hybrides éprouvées.**
   Adoptez les meilleures pratiques des secteurs réglementés qui ont géré efficacement des environnements hybrides. Investissez dans l'intégration sécurisée de l'infrastructure cloud privée et publique afin de débloquer et d'exploiter les 90 % de données privées essentielles à l'IA de nouvelle génération.

Chapitre huit

Mettre l'IA agentique au travail

Dans ce chapitre, nous verrons comment mettre l'IA au service de votre entreprise. Un cadre efficace nécessite de comprendre les trois niveaux de l'IA : l'IA générative, qui crée et synthétise, l'IA agentique, qui prend des décisions et agit, et l'intelligence artificielle générale, qui étend le raisonnement sur plusieurs domaines, comme l'esprit humain. Ensemble, ces couches constituent la base des systèmes d'intelligence artificielle d'entreprise intelligents et adaptatifs.

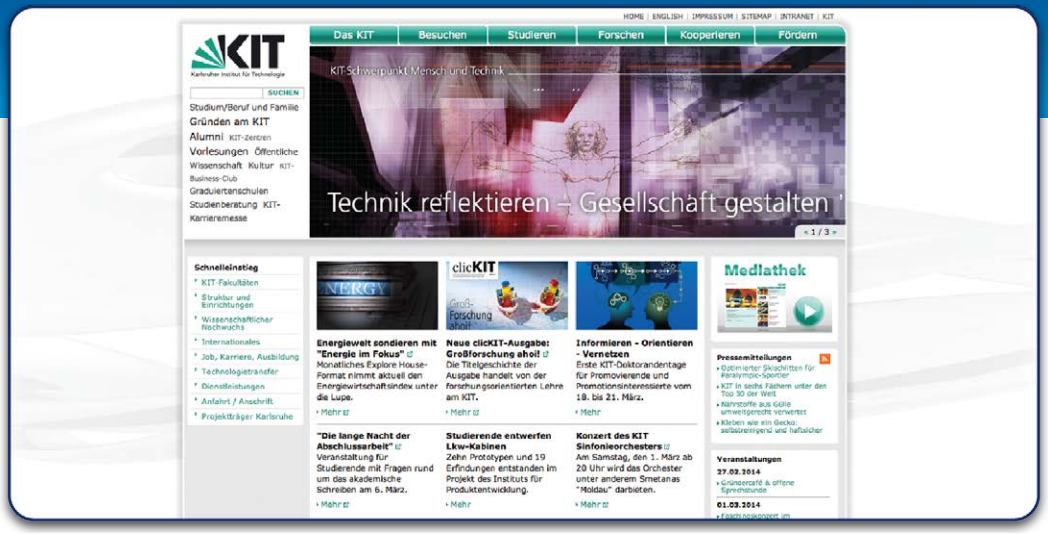
L'IA d'entreprise a depuis longtemps dépassé le stade de la nouveauté. Les entreprises n'expérimentent plus de simples générateurs de texte ou n'utilisent plus l'IA pour rédiger les lignes d'objet des courriels. L'accent a été mis sur des outils isolés plutôt que sur des collaborateurs autonomes travaillant aux côtés des personnes. Il s'agit d'agents IAE : des entités logicielles intelligentes qui non seulement génèrent des résultats, mais agissent, réagissent et s'adaptent au sein d'environnements commerciaux dynamiques. Contrairement aux applications d'IA traditionnelles qui répondent à des demandes statiques, les agents IAE fonctionnent davantage comme des collègues numériques : ils exécutent des flux de traitement en plusieurs étapes, participent à la résolution de problèmes contextuels et soutiennent les opérations quotidiennes avec rapidité, cohérence et intelligence. La différence est subtile mais profonde : cette nouvelle classe d'IA ne se contente pas de répondre aux questions, elle fait le travail.

Les agents IAE vont au-delà des outils d'efficacité pour devenir des multiplicateurs de force pour l'entreprise. Toujours disponibles, d'une précision constante et de plus en plus aptes à saisir les nuances, ils apportent une amélioration mesurable sans augmenter les frais généraux. Qu'il s'agisse d'automatiser les flux de travail, de gérer les interactions avec les clients, d'analyser des ensembles de données complexes ou de guider les utilisateurs lors de l'intégration, les agents IAE apportent précision et évolutivité aux opérations de routine. Leur fiabilité garantit des expériences uniformes, tandis que leur rapidité transforme de vastes données en informations pertinentes. Le résultat va au-delà d'une simple réduction des coûts : il s'agit d'une capacité retrouvée pour se concentrer sur la stratégie, l'innovation et la croissance.

Grâce à l'intégration de la GIE et de l'IAE, les entreprises du secteur public telles que l'Institut de technologie de Karlsruhe (KIT) disposent de capacités d'analyse de pointe, conçues pour extraire, extraire et présenter la véritable valeur des informations afin d'améliorer la recherche et l'analyse. Découvrez-le dans l'étude de cas suivante.

Étude de cas

Institut de technologie de Karlsruhe



Institut de technologie de Karlsruhe (KIT)

L'Institut de technologie de Karlsruhe (KIT), l'un des principaux instituts de recherche en ingénierie au monde, a été fondé en 2009 par la fusion du Forschungszentrum Karlsruhe et de l'Universität Karlsruhe. En tant que membre de l'association Helmholtz, la plus grande organisation scientifique d'Allemagne, le KIT apporte une contribution majeure à la recherche nationale et internationale de pointe. Conformément à sa mission, l'organisation opère dans trois domaines d'action stratégiques : la recherche, l'enseignement et l'innovation. Le KIT compte actuellement 9 000 employés et 24 000 étudiants.

Le KIT avait besoin d'une solution de pointe qui permettrait aux chercheurs, aux étudiants et au grand public de trouver plus rapidement des informations sur 600 sites Web et 200 000 pages Web associées. En arrière-plan, l'institut recherchait une solution de gestion de site Web robuste capable de prendre en charge au quotidien ses 1 300 rédacteurs dispersés dans le monde entier, en fournissant des métadonnées, des phrases clés et la possibilité de générer automatiquement des extraits de texte. Le KIT souhaitait également une plateforme collaborative réunissant des chercheurs, des scientifiques et des étudiants.

Le KIT utilise les technologies de l'administration gouvernementale en ligne, la navigation sémantique et l'analyse de contenu, en combinaison avec la gestion de sites Web, afin d'optimiser les pages Web et de fournir des résultats de recherche pertinents. Les tâches manuelles qui exigeaient auparavant beaucoup de travail ont été remplacées par une solution automatisée qui attribue des métadonnées et permet l'extraction d'entités en générant des textes d'accroche pour les nouvelles pages, ce qui permet aux utilisateurs de gagner du temps et de réduire les erreurs. Les visiteurs bénéficient d'un accès personnalisé à des informations hautement pertinentes, facilité par une recherche à facettes et des résultats connexes, ce qui se traduit par une expérience utilisateur finale plus satisfaisante. Grâce à un meilleur accès à l'information et à la possibilité d'entrer en contact avec des chercheurs travaillant dans des domaines similaires, le site Web est devenu un réseau de recherche avancé qui répond efficacement aux besoins de tous les groupes de parties prenantes.

Trois niveaux d'IA

L'IA générative (GenAI) a gagné en popularité auprès des consommateurs grâce à des modèles tels que ChatGPT d'OpenAI et Gemini de Google. Ces derniers, comme d'autres modèles linguistiques étendus (MLE) et applications d'IA, sont formés pour faire des prédictions ou des recommandations basées sur des sources de données accessibles au public, notamment les sites Web, les actualités, Reddit et Wikipedia, entre autres. Bien que les modèles GenAI soient utiles pour générer des informations générales, ils sont limités aux tâches générales. En effet, ils n'ont pas accès aux données privées, en temps réel et centrées sur l'entreprise qui sont nécessaires pour des cas d'utilisation spécifiques.

L'IA agentique fait référence aux systèmes d'intelligence artificielle conçus pour fonctionner comme des agents autonomes. Contrairement aux modèles qui répondent simplement à une demande, un agent peut percevoir son environnement, créer un plan en plusieurs étapes, prendre des décisions indépendantes et utiliser des outils pour travailler activement à un objectif précis.

Dans un contexte d'entreprise, ces agents constituent un puissant moteur de productivité, les données servant de carburant. Ils peuvent avoir accès à des ensembles de données d'entreprises privées et à des outils internes, ce qui leur permet d'automatiser des flux de traitement complexes qui nécessitaient auparavant un jugement humain. L'IA agentique est alimentée par un « cerveau numérique », un modèle unique et compétent capable de traiter des décennies de réponses humaines.

Cette technologie est déjà en train de transformer les industries, et les entreprises qui ne parviendront pas à adopter et à orchestrer l'IA agentique seront distancées. C'est également une voie vers l'intelligence générale artificielle (IAG).

L'intelligence générale artificielle (IAG) fait référence à une IA capable de comprendre, d'apprendre et d'appliquer des connaissances dans le cadre d'un large éventail de tâches complexes, un peu comme les humains. 53 Une telle technologie serait capable de redéfinir non seulement des secteurs, mais des sociétés entières.

Comme toute intelligence artificielle moderne, les capacités d'une éventuelle IAG seraient fondamentalement façonnées par la qualité et l'ampleur de ses données d'entraînement. Les fondements de l'IAG proviendront probablement de l'orchestration de milliers d'instances agentiques spécialisées d'IA dans un cadre sécurisé et souverain, comme décrit au chapitre 7.

Développer l'IA agentic pour l'entreprise

Des données fiables et des processus commerciaux efficaces sont essentiels pour obtenir des résultats optimaux en matière d'IA, et l'inverse est également vrai. Grâce à la protection des données d'entreprise et aux grands modèles linguistiques (MLE) affinés à l'intérieur de votre domaine, tout est prêt pour créer ce que nous appelons des « capacités agentiques » qui offrent une réelle valeur commerciale.

L'IA agentique ne se limite pas à la technologie ; il s'agit de renforcer les capacités de vos processus commerciaux et de soutenir une combinaison de personnes, de processus, de culture et de gestion du changement. Si c'est bien fait, cela devient bien plus qu'une expérience de production générative. Plutôt que de simplement demander à un modèle de « résumer un document », l'intelligence artificielle agentique peut détecter un goulot d'étranglement dans un flux de travail, diviser les tâches en sous-tâches, appeler des API ou d'autres systèmes pour les exécuter, surveiller les résultats, en tirer des leçons, puis affiner l'étape suivante avec un minimum de directives humaines.

Prenons les conclusions de l'initiative NANDA du Massachusetts Institute of Technology (« The GenAI Divide : State of AI in Business 2025 ») : environ 5 % seulement des projets pilotes d'IA générative en entreprise ont enregistré une croissance rapide des revenus ; les 95 % restants n'ont pas eu d'impact mesurable sur les résultats financiers. Selon les chercheurs, l'obstacle n'était pas le modèle ou le matériel, mais le « déficit d'apprentissage » ou l'incapacité des systèmes d'IA et des flux de traitement organisationnels à s'adapter ensemble. [54]

Parmi les leçons tirées : affecter les investissements dans l'IA là où ils s'alignent sur des processus spécifiques, et pas seulement sur des cas d'utilisation très visibles ; intégrer des boucles de feedback pour que le système apprenne ; intégrer en profondeur les opérations existantes plutôt que de se contenter d'un outil générique ; et veiller à ce que la gestion du changement soit en place afin que les personnes et la culture accueillent favorablement le changement. En bref : lorsque la qualité des données, l'alignement des processus, le niveau de préparation de l'entreprise et la modélisation spécifique à un domaine convergent, votre entreprise est en mesure de passer d'un projet pilote à une véritable création de valeur basée sur l'IAE.

Les arguments en faveur de l'IA agentique

Les entreprises adoptent de plus en plus l'IA en réponse aux pressions liées aux changements économiques et technologiques rapides, notamment la nécessité d'une transformation numérique, de nouveaux modèles commerciaux, d'une prise de décision en temps réel, d'une envergure mondiale et de la capacité à s'adapter aux perturbations. [55] Les agents IA, capables d'exécuter des tâches de manière semi-autonome ou totalement autonome, les aident à rester compétitifs, à faire évoluer les flux d'informations, à réduire la charge cognitive des humains et à améliorer leur agilité.

Le déploiement de systèmes d'agents d'intelligence artificielle n'est qu'un début. Le plus grand défi consiste à les soutenir et à s'assurer qu'ils continuent à apporter de la valeur, à rester alignés sur les objectifs de l'entreprise et à évoluer au même rythme que l'écosystème homme-machine. [56] Il est essentiel de commencer par des processus métier bien connus, et cela sera traité plus en détail dans le chapitre suivant. Il est préférable d'adopter une approche basée sur des normes et de commencer par identifier des tâches simples et discrètes pour vos premiers agents. Cette méthode jettera les bases d'un modèle orchestré plus complexe à l'avenir.

L'article suivant sur une Cour européenne des droits de l'homme montre comment la GIE aide à consolider les informations afin de garantir l'exactitude et l'intégration de l'IA dans les processus clés, réduisant ainsi la charge administrative et améliorant les performances. Par conséquent, les agences sont mieux équipées pour accomplir leur mission de protection des citoyens.

Étude de cas

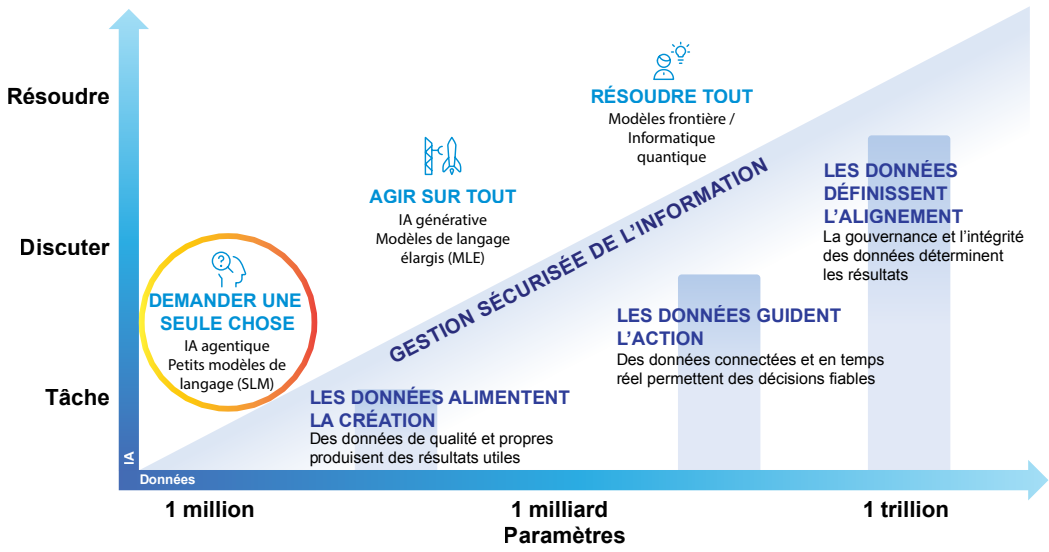
Une cour européenne

La Cour fait partie du Conseil de l'Europe, une organisation intergouvernementale internationale créée en 1949 pour promouvoir la démocratie politique et les droits de l'homme, le progrès social et l'identité culturelle sur tout le continent.

Au cours de la dernière décennie, la Cour a vu sa charge de travail fortement augmenter, passant de 14 000 requêtes à plus de 50 000. Pour gérer cette augmentation, le service informatique de la Cour a conçu une solution de flux de traitement automatisé qui a rationalisé le processus d'approbation des affaires des comités et des chambres. Ce qui a commencé comme une initiative de transformation numérique s'est depuis transformé en un écosystème d'informations intelligent, alimenté par l'analytique, la GIE et maintenant, l'IA agentique.

Aujourd'hui, les flux de traitement de la Cour ne se contentent pas d'acheminer des documents : ils raisonnent, s'adaptent et agissent. Construit sur une base de données gouvernées, le système utilise l'analytique pour identifier les goulots d'étranglement des processus et l'IA agentique pour les optimiser en temps réel. Par exemple, la plateforme peut détecter les cas où l'examen d'un dossier est trop long, le signaler automatiquement pour escalade et redistribuer la charge de travail entre les divisions afin de maintenir le débit. Les assistants juridiques ne passent plus des heures à chercher des traces écrites. L'IA suit les progrès, génère des rapports dynamiques et recommande les prochaines étapes, en tirant continuellement des enseignements des résultats pour améliorer les décisions futures en matière d'itinéraire.

Les résultats parlent d'eux-mêmes : des délais de traitement des affaires plus courts, moins de blocages administratifs et plus de temps pour que les experts juridiques de la Cour puissent se concentrer sur l'interprétation plutôt que sur l'administration. Grâce à l'analyse, à la GIE et à l'IA agentique travaillant de concert, la Cour est passée d'une institution réactive à une institution proactive, prête à évoluer, à s'adapter et à rendre justice à la vitesse exigée par les charges de travail modernes.



Ces informations forment toutes les formes d'IA

Des bases de données solides

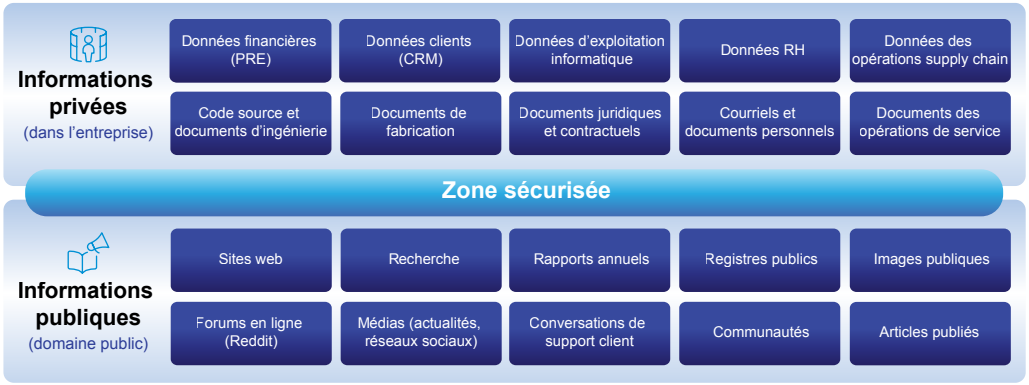
Le principal défi consiste à tirer parti de données sécurisées et de haute qualité pour obtenir des résultats en matière d'intelligence artificielle et atteindre son plein potentiel. Comme l'illustre le schéma ci-dessus, il existe un lien direct entre de solides bases de données et des résultats réussis en matière d'IA.

Au-delà des données, une stratégie efficace doit également tenir compte de l'infrastructure. Les différents modèles d'IA ont des exigences différentes, et les données et l'architecture de l'IA doivent être conçues pour adapter le bon modèle à la bonne tâche commerciale.

Débloquer des données privées pour soutenir l'IA agentique

Compte tenu de la qualité et de la quantité des données d'entreprise qui se trouvent derrière le pare-feu, il est essentiel de tirer parti de ces données privées. C'est en peaufinant ou en adaptant un MLE avec ces connaissances spécifiques à ce domaine que l'IA agentique peut gérer des cas d'utilisation commerciale et d'application significatifs et réels.

Les pipelines de données, le lignage des données et les flux de données deviendront essentiels. Chaque entreprise devra devenir une société d'entrepôt de données. Lorsque nous examinons l'étendue des données au sein de l'entreprise, il est clair que le déverrouillage de l'IA nécessite une stratégie permettant de travailler à la fois sur les ensembles de données publics et privés, qui font chacun partie intégrante du mode de fonctionnement actuel de chaque entreprise des secteurs privé et public. Le schéma suivant illustre des exemples de ces ensembles de données.



Exemples de jeux de données

Tirer parti des données privées pour affiner les MLE

Les grands modèles linguistiques s'appuient sur d'importantes quantités de données pour s'entraîner. Ils tirent des leçons des modèles contenus dans ces données, notamment des mots, des phrases, de la syntaxe et des relations sémantiques. [57]

Bien que la qualité et l'échelle de ces données de formation initiale soient importantes, leur pertinence est essentielle pour une utilisation en entreprise. Comme indiqué précédemment, les MLE formés par le public (comme ceux d'OpenAI, Cohere ou Anthropic) sont excellents pour les tâches générales, mais manquent de contexte détaillé lorsqu'il s'agit d'entreprises spécifiques. Pour pallier cette limite, les entreprises ont désormais recours à de multiples stratégies d'adaptation pour aligner les modèles sur leurs données et environnements propriétaires. La plus connue d'entre elles est le réglage fin, tandis que des techniques telles que l'ingénierie contextuelle offrent une flexibilité et une rapidité complémentaires.

Pour affiner un modèle de base, il faut utiliser le modèle pré-formé publiquement et poursuivre sa formation sur un ensemble de données plus petit, spécifique au domaine ou propriétaire. Cela permet au modèle d'apprendre le vocabulaire, les données et les processus uniques de l'entreprise sans exposer ces données privées au public. Ce réglage précis fournit un modèle dérivé personnalisé qui est plus performant pour les tâches spécifiques à l'entreprise et au domaine, car il a internalisé les modèles issus des données privées. [58]

Parallèlement, l'ingénierie contextuelle permet aux entreprises d'affiner le comportement du modèle de manière dynamique en structurant et en mettant à jour le contexte d'entrée (par exemple, des prompts, des exemples ou des métadonnées) plutôt que de réentraîner le modèle. Cette approche permet une adaptation plus rapide et moins coûteuse, prend en charge le désapprentissage sélectif pour des raisons de confidentialité ou de conformité légale, et est particulièrement utile lorsque vous travaillez avec des modèles à source fermée. [59]

Dans la pratique, les entreprises combinent souvent les deux approches : ajustement précis pour un alignement approfondi des domaines et des performances à long terme, et ingénierie du contexte pour une adaptation agile en temps réel. Ensemble, ils créent une stratégie durable à plusieurs niveaux pour aligner les MLE sur les objectifs de l'entreprise et les normes de conformité. [60]

Dans l'article suivant, un leader des technologies de voyage en matière de forfaits vacances dynamiques permet aux vacanciers d'accéder à des millions de combinaisons en temps réel. Il utilise la technologie pour simplifier, personnaliser et améliorer les expériences de voyage des clients.

Étude de cas

Une entreprise de technologie du voyage

Alors que ses activités se développent sur plusieurs marchés européens et que la demande de forfaits vacances en temps réel augmente, une entreprise spécialisée dans les technologies du voyage a connu une augmentation soutenue du volume et de la variété de ses données. Les réservations, les interactions Web, les flux de partenaires, les activités marketing et les engagements de support client ont tous généré des données à haute vitesse avec des structures et des exigences de latence différentes. Cette croissance a menacé la poursuite des initiatives en matière de gouvernance, de modèle d'accès et de délai d'obtention d'informations.

Au fil du temps, le parc de données s'est scindé en deux silos : un entrepôt de données doté d'outils ETL (Extract, Transform, Load) et de création de rapports, et un data lake pour l'ingestion de données brutes. Cette séparation a entraîné des doublons, des frais de maintenance et un ralentissement des analyses. Les équipes se sont appuyées sur différents outils et sur un code « collé » personnalisé pour combler le fossé entre les systèmes, ce qui a créé un « clivage marqué » qui a rendu la croissance plus difficile et a ralenti la diffusion des informations.

L'entreprise a adopté une couche d'accès aux données unifiée, éliminant ainsi les pipelines d'ingestion séparés et le besoin d'un code adhésif complexe. Grâce à une interface commune et à un ensemble d'outils partagés, les ingénieurs et les analystes pouvaient interroger et traiter les données de manière cohérente dans tous les systèmes. En fusionnant les environnements et en dissociant les producteurs des consommateurs, tout en préservant une compatibilité totale, l'entreprise a obtenu une source unique de vérité. Cette intégration a permis des analyses plus riches, en corrélant les données de veille commerciale avec les informations relatives au marketing, au CRM et à l'apprentissage automatique pour alimenter des modèles clients avancés et prédictifs.

L'entreprise est ensuite passée à un environnement de cluster conteneurisé utilisant Kubernetes pour automatiser le déploiement, le dimensionnement et la gestion de la charge de travail. Les tâches de requête peuvent désormais être exécutées à la demande et s'arrêter une fois terminées, grâce à un stockage partagé et à un calcul adapté à chaque tâche, qu'il s'agisse de l'ETL ou des tableaux de bord analytiques. Le résultat : une évolutivité et une efficacité accrues, avec une réduction des coûts de calcul, de la consommation d'énergie et de l'empreinte carbone.

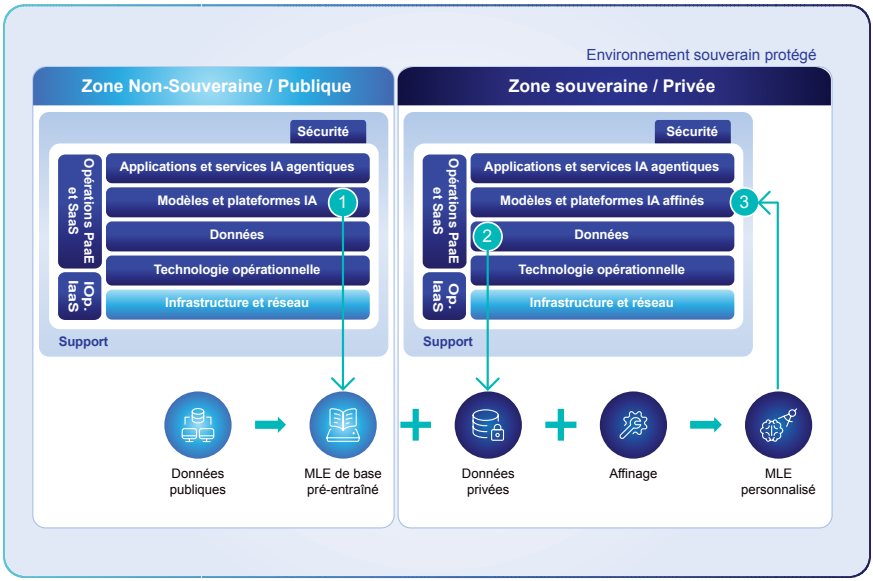
L'entreprise est en mesure d'étudier le comportement des clients sur tous ses canaux et d'analyser chaque étape du parcours client, des recherches préliminaires au paiement final. La mise en œuvre a un impact positif sur le retour sur investissement (ROI) des campagnes marketing et sur le chiffre d'affaires de l'entreprise. En outre, les algorithmes basés sur l'IA pour l'attribution et l'automatisation des enchères aident à optimiser les coûts marketing globaux, ce qui se traduit par une augmentation des profits.

Mais puis-je garantir la souveraineté de mes données privées et un modèle affiné ?

C'est là le cœur du défi. Vos données, et l'IA qui en découle, constituent votre avantage concurrentiel. La qualité de vos données définit l'efficacité et l'intégrité de votre MLE. Cependant, une fois que vous avez formé un MLE sur un ensemble de données spécifique, il ne peut pas désapprendre ces données.

C'est l'une des principales raisons pour lesquelles les données privées et l'IA privée sont essentielles. Lorsque vous entraînez un modèle, celui-ci internalise les modèles de données et en fait une marque indélébile. Ces apprentissages sont interconnectés avec d'autres données, dans le cadre à la fois des exemples spécifiques et de la distribution plus large des données sous-jacentes. Pour cette raison, toute tentative de désapprentissage de données d'entraînement spécifiques nécessite un nettoyage massif des paramètres et des connexions qui déterminent le comportement du modèle. Dans « Machine Unlearning Doesn't Do What You Think : Lessons for Generative AI Policy, Research, and Practice », les auteurs soulignent que « la suppression d'informations d'un modèle de ML [apprentissage automatique] n'est pas bien définie. Tout d'abord, les informations ne peuvent pas être supprimées d'un modèle d'apprentissage machine de la même manière qu'elles le peuvent d'une base de données. »[61]

Bien que des travaux soient en cours pour affiner les approches du « désapprentissage automatique », il ne s'agit pas d'une voie simple pour une entreprise du secteur privé ou public. La nécessité de protéger les données souveraines ou privées et le modèle qui en résulte est primordiale.



Architecture souveraine des données et de l'IA

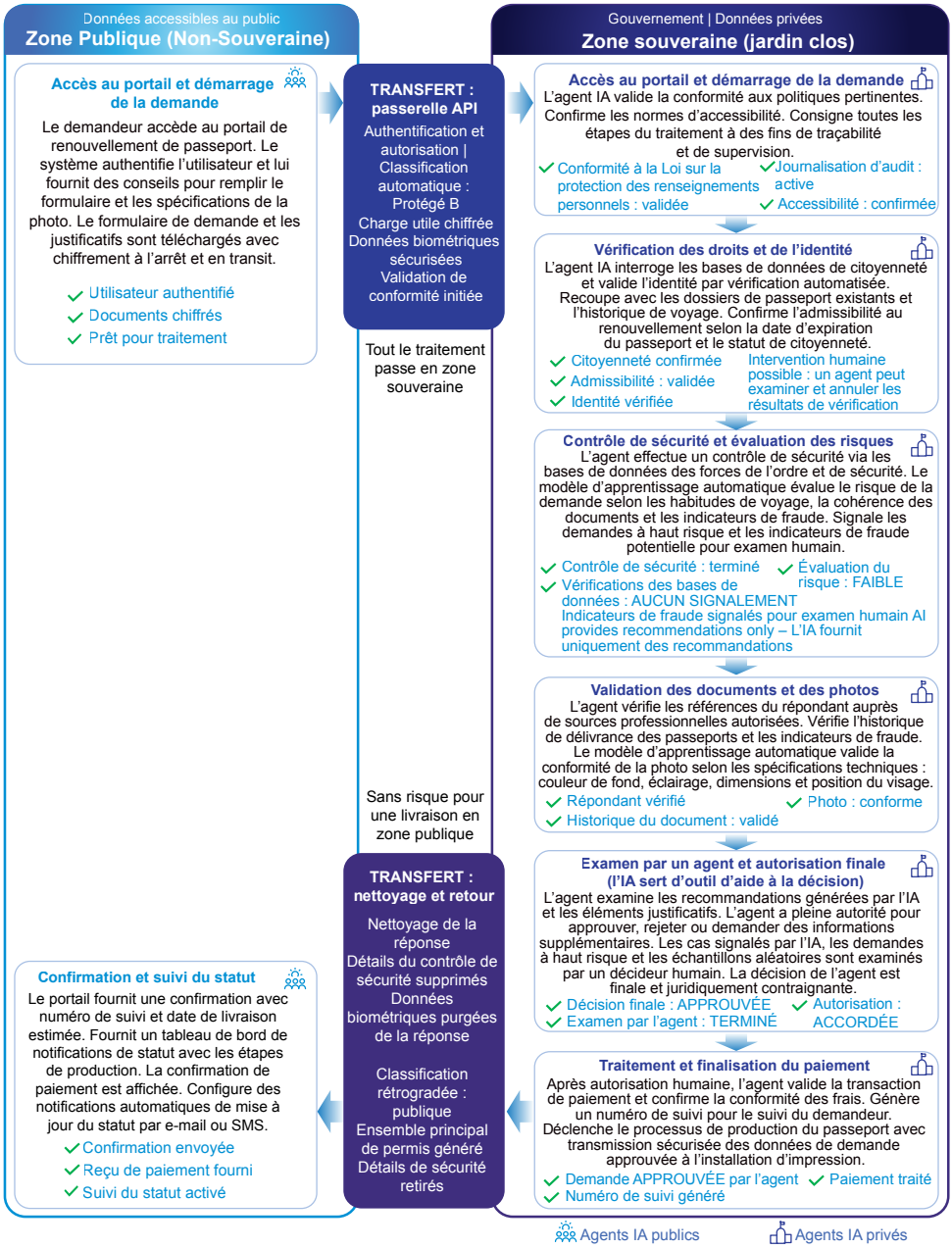
C'est précisément pourquoi une architecture souveraine en matière de données et d'intelligence artificielle est si essentielle. Au lieu de miser sur le désapprentissage, cette approche repose sur la prévention. Elle est conçue pour préserver la confidentialité de vos données et du modèle affiné dès le départ. Cela nécessite de s'assurer que le modèle est déployé dans une zone souveraine certifiée où vos modèles affinés sont protégés, comme illustré dans l'architecture ci-dessus.

Dans la figure ci-dessus, les données publiques sont utilisées pour fournir un MLE de base pré-formé (1) qui fonctionne dans la zone non souveraine/publique. Un ensemble complet de fonctionnalités d'intelligence artificielle agentique peut être fourni dans cet environnement. Du côté de la zone privée, le modèle de base est affiné avec des données privées (2), qui fournissent à leur tour un MLE personnalisé qui inclut des spécificités du domaine ou du secteur qui peuvent être un facteur de différenciation pour votre entreprise. Ce MLE (3) peut être exploité par une IA agentique opérant dans la zone privée, et les données ne sont pas renvoyées au MLE opérant dans la zone publique.

En particulier, si vous contrôlez l'infrastructure sur laquelle le modèle est déployé, vous pouvez garder ce modèle privé. Si le modèle est hébergé dans le cloud public, vous avez besoin de garanties de la part du fournisseur de cloud public et du fournisseur du modèle (s'ils sont différents) quant à la souveraineté de vos données.

L'IA agentique dans un contexte souverain : un cas d'utilisation

Si nous situons l'IA agentique dans le contexte de la souveraineté, nous pouvons utiliser un exemple familier aux citoyens de nombreux pays : la demande d'un nouveau passeport. Cet exemple met en évidence le besoin d'ensembles de données privés et publics, et montre comment l'IA agentique peut naviguer dans les deux environnements, avec des modèles affinés fonctionnant dans le monde souverain/privé fonctionnant aux côtés de modèles déployés dans la zone non souveraine/publique. Lorsque ces environnements fonctionnent ensemble, le client final est le bénéficiaire final, qui bénéficie d'une expérience nettement améliorée.



Cas d'utilisation du traitement des passeports comprenant des zones souveraines et des zones non souveraines

Étape 1 : Accès au portail et démarrage de l'application (zone publique)
Le demandeur commence par accéder à un portail de renouvellement de passeport. Le système authentifie l'utilisateur et fournit des conseils sur la façon de remplir et de soumettre la demande. Les informations de passeport et les pièces justificatives sont téléchargées de manière cryptée à la fois au repos et en transit. À ce stade, les statuts incluent l'authentification de l'utilisateur, le chiffrement des documents et la préparation au traitement.

Étape 2 : transfert — API Gateway
La passerelle API gère l'authentification et l'autorisation, en classant automatiquement les données comme étant protégées. La charge utile est cryptée, les données biométriques sont sécurisées et la validation de conformité est lancée.

Étape 3 : Conformité et validation des politiques (zone souveraine)
L'agent IA du gouvernement vérifie la conformité avec les réglementations et politiques pertinentes en matière de confidentialité et d'information.

Le système confirme la capacité des services linguistiques et les normes d'accessibilité, en enregistrant toutes les étapes de traitement à des fins de suivi et de conformité. À ce stade, les statuts incluent la validation de la conformité, la journalisation active des audits et la confirmation de l'accessibilité.

Étape 4 : Vérification de la citoyenneté et de l'identité (zone souveraine)
L'agent d'intelligence artificielle du gouvernement interroge la base de données de citoyenneté pour vérifier que l'identité correspond à celle figurant dans la demande de passeport soumise. Il recoupe les dossiers de passeport existants pour confirmer l'éligibilité en fonction de la nationalité et d'autres critères. Les statuts incluent la citoyenneté confirmée, la possibilité d'annuler le match si nécessaire et l'éligibilité validée.

Étape 5 : Contrôle de sécurité et évaluation des risques (zone souveraine)
L'agent d'intelligence artificielle du gouvernement effectue des contrôles de sécurité par le biais de bases de données des forces de l'ordre, en utilisant les habitudes de voyage et les facteurs de risque. Les modèles d'apprentissage automatique évaluent les risques liés aux applications en fonction des habitudes de voyage et recoupent les listes de surveillance, puis fournissent des alertes pour une révision manuelle si nécessaire. Les statuts incluent un contrôle de sécurité effectué et une évaluation des risques classée comme faible, moyen ou élevé.

Étape 6 : Validation des documents et des photos (zone souveraine)
L'agent d'intelligence artificielle du gouvernement valide les informations d'identification des garants par le biais d'une recherche dans la base de données, vérifie l'historique des passeports pour détecter les problèmes ou les indicateurs de fraude liés aux voyages, et utilise des modèles d'apprentissage automatique pour authentifier la photo par rapport aux dossiers d'identité et aux bases de données gouvernementales. Les statuts incluent les informations d'identification validées du garant et l'intégrité vérifiée des documents.

Étape 7 : Examen par un agent et autorisation finale (zone souveraine)
Un agent humain expert examine toutes les informations signalées par le système, en utilisant l'IA comme outil d'aide à la décision. L'agent humain accorde l'autorisation finale sur la base de l'examen complet de toutes les informations validées. Ce flux de traitement garantit que les données personnelles sensibles sont gérées, validées et traitées en toute sécurité conformément aux réglementations en matière de confidentialité, en maintenant une séparation claire entre les zones publiques et souveraines.

Bien que les cas d'utilisation spécifiques puissent varier, et il s'agit d'un exemple simplifié, il met en évidence la manière dont l'engagement de l'IA agentique interagit entre les zones souveraines et non souveraines tout en gérant des informations personnelles identifiables dans le cadre d'un déploiement hybride. La mise en œuvre et la gestion du déploiement de l'IA agentique nécessitent une prise en compte plus large de la manière dont les agents numériques et le personnel humain travaillent de concert. L'IA agentique exécute les tâches en utilisant sa logique intégrée, tandis que la supervision humaine garantit des résultats positifs.

Le chapitre suivant étudiera plus en profondeur la manière dont les effectifs numériques et humains doivent travailler de concert pour exploiter le potentiel de l'IA dans l'entreprise.

Lisez l'article suivant pour découvrir comment le Conseil général de la magistrature utilise un système GIE fiable pour consolider en toute sécurité les informations publiques et privées, afin d'améliorer la prestation de ses services aux citoyens espagnols.

Étude de cas

Conseil général de la magistrature

Poderjudicial.es

> *ALes analyses nous aident à mesurer le succès de nos services et les performances globales du site public, en nous fournissant les outils dont nous avons besoin pour présenter aux utilisateurs une expérience réactive, soutenue par du contenu multimédia.*

Le Conseil général du pouvoir judiciaire (Consejo General del Poder Judicial ou CGPJ) a été créé par la Constitution espagnole en 1978 en tant qu'organe constitutionnel qui régit le pouvoir judiciaire en Espagne. Le CGPJ souhaitait combiner ses systèmes dans un portail en ligne afin de fournir aux citoyens un accès personnalisé aux informations et aux services dont ils ont besoin.

Le nouveau portail prendrait en charge une variété de canaux de communication dans plusieurs langues. En arrière-plan, le système devrait intégrer tous les services corporatifs du Conseil judiciaire afin de rationaliser la collaboration, de fournir des services intégrés tels que les applications en ligne, de permettre la gestion sécurisée des informations et de se conformer aux réglementations en vigueur en matière de transparence, d'accessibilité, de multilinguisme, de loi 11/2007, etc.

Une solution d'administration en ligne a été choisie comme base pour le site Web et l'extranet judiciaire du CGPJ, fournissant au Conseil une plateforme techniquement solide et gérable pour l'avenir. Le portail multilingue prend en charge un nombre important de visites et est facilement évolutif. Le processus de publication sur le Web est plus efficace ; les fonctionnalités de libre-service ont considérablement réduit le temps nécessaire pour publier des informations actualisées.

Le système a été mis en ligne en interne avec 6 500 utilisateurs actifs et 5 400 messages échangés sur ses forums. Les membres de la magistrature peuvent participer et collaborer en utilisant les environnements virtuels du système, les 45 communautés de pratique et les fichiers partagés. L'accès sécurisé aux applications et services intégrés est assuré par le biais de l'authentification unique et de la gestion des identités. Le système est personnalisable, ce qui permet aux utilisateurs de personnaliser et de configurer leur environnement de travail.

Télécharger The Fast Five

1. **Déployez l'IA agentique pour créer de la valeur pour l'entreprise.**
   Accélérez la productivité et l'adaptabilité en adoptant des applications d'intelligence artificielle agentiques qui perçoivent, planifient, décident et agissent de manière autonome, ce qui permet d'automatiser des flux de traitement complexes et de réduire la dépendance à l'égard des interventions manuelles.

2. **Tirez parti des données privées spécifiques à un domaine pour vous différencier.**
   Bénéficiez d'un avantage commercial en affinant les modèles d'IA avec les données internes propriétaires de votre entreprise, en donnant à l'IA agentique les moyens de résoudre des problèmes spécifiques à un domaine que les modèles génériques ne peuvent pas résoudre et en établissant une base de données sécurisée et de haute qualité.

3. **Mettez en œuvre des architectures d'IA souveraines pour protéger la propriété intellectuelle et la confidentialité.**
   Protégez les données sensibles et la propriété intellectuelle de votre entreprise en déployant des modèles d'IA dans des environnements sécurisés et souverains, afin de garantir la conformité, la confidentialité des données et le contrôle total de vos actifs d'IA.

4. **Concentrez les initiatives d'IA sur des systèmes ciblés et capables d'apprentissage.**
   Maximisez le retour sur investissement en orientant l'IA agentique vers des processus métier spécifiques et bien compris, et en investissant dans des systèmes qui apprennent et s'adaptent au fil du temps, en évitant les solutions génériques et en minimisant les changements organisationnels perturbateurs.

5. **Favorisez la collaboration homme-IA pour un impact durable.**
   Garantissez une valeur continue en établissant des normes de supervision humaine et d'alignement, en commençant par de simples tâches agentiques, et en cultivant une collaboration homme-machine efficace qui évolue en fonction des besoins de votre entreprise.

Chapitre neuf

La gestion des applications IAE

Dans les entreprises d'aujourd'hui, la gestion des applications d'intelligence artificielle ne consiste plus à déployer un modèle unique, mais à orchestrer une symphonie d'agents intelligents opérant dans des zones publiques et souveraines, des clouds privés et des réseaux ouverts, ainsi qu'à travers une multitude de flux de travail. Il s'agit de l'intelligence artificielle d'entreprise et la gestion de cette complexité ne se limite pas à des prouesses techniques ; elle nécessite une approche organisationnelle sophistiquée ancrée dans des processus commerciaux, une gestion du changement et une gouvernance solides. Comme l'indiquent des recherches récentes, les entreprises hésitent à appliquer l'IA non pas parce que les modèles sont inadéquats, mais parce que leurs structures, leurs propriétaires et leurs flux de traitement ne sont pas prêts à cela.

Dans ce chapitre, nous exposons les principes clés qui garantissent que votre entreprise peut non seulement déployer l'IA agentique, c'est-à-dire des systèmes qui raisonnent, planifient, agissent et collaborent, mais également les gérer d'une manière conforme aux objectifs stratégiques, aux cadres de risque et à la gouvernance centrée sur l'humain.

Ces quatre principes définissent les bonnes conditions pour un déploiement réussi des systèmes d'IA agentique d'entreprise :

1. **Modèle organisationnel pour les déploiements d'IAE agentiques** : garantir que la propriété et la responsabilité, ainsi que les rôles et les responsabilités, sont clairs.
2. **Développement d'applications d'IAE agentique** : Adopter une approche structurée pour prioriser et renforcer les capacités de l'entreprise.
3. **Collaboration entre les équipes humaines et d'IAE agentique** : veiller à ce que vos équipes adoptent et adoptent l'IA avec une définition claire du rôle et de l'objectif.
4. **Gestion et mesure des performances** : Fermer la boucle de rétroaction en mesurant les résultats et en gérant les performances de votre personnel d'IA agentique.

Au fur et à mesure que nous aborderons chacun de ces principes, vous découvrirez des cadres, des meilleures pratiques et des considérations concrètes pour créer et exploiter l'IA d'entreprise à grande échelle. De la définition du modèle de l'organisation à la conception de flux de travail partagés par les humains et les agents, en passant par la mesure de la valeur et l'adaptation continue, ce chapitre vous permet de passer d'expériences d'IA isolées à des déploiements à l'échelle de l'entreprise. Commençons par découvrir comment le modèle organisationnel jette les bases d'applications d'IA responsables et évolutives.

1. Un modèle organisationnel pour les déploiements d'IA agentique

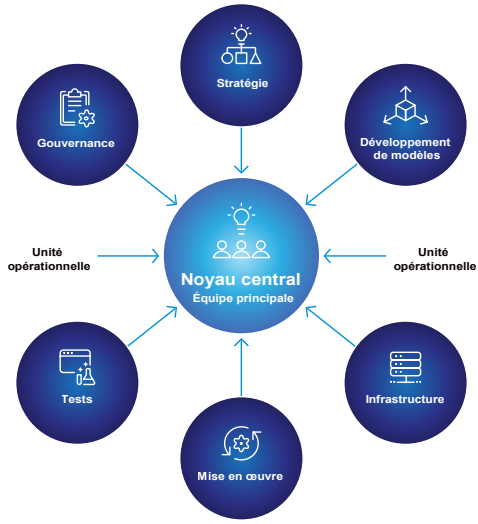
Comment choisir le bon modèle

Les entreprises qui cherchent à favoriser l'adoption de l'IA, et plus particulièrement à fournir des capacités d'IA agentiques, doivent prendre une décision critique quant à la manière de gérer leurs applications d'IA. Il existe plusieurs modèles courants, chacun avec des attributs positifs et négatifs distincts, mais l'aspect le plus crucial est de choisir le bon.

Les exemples suivants décrivent quatre modèles qui fonctionnent dans différentes organisations en fonction du secteur et du niveau de réglementation : modèle centralisé (centre d'excellence en intelligence artificielle/COE), modèle noyau et rayons, modèle fédéré et modèle hybride.

Le modèle centralisé

Dans ce modèle, une équipe centralisée possède des compétences approfondies et est chargée de piloter la stratégie, le développement du modèle, l'infrastructure, la mise en œuvre, les tests et la gouvernance. Cela garantit la cohérence et le contrôle, ainsi qu'une gouvernance unifiée ; toutefois, cela peut exonérer les unités commerciales de toute responsabilité quant à l'obtention de résultats grâce à leur adoption de l'IA. De nombreuses entreprises novices en matière d'adoption des technologies, ainsi que celles des secteurs réglementés et du gouvernement, trouvent ce modèle intéressant.

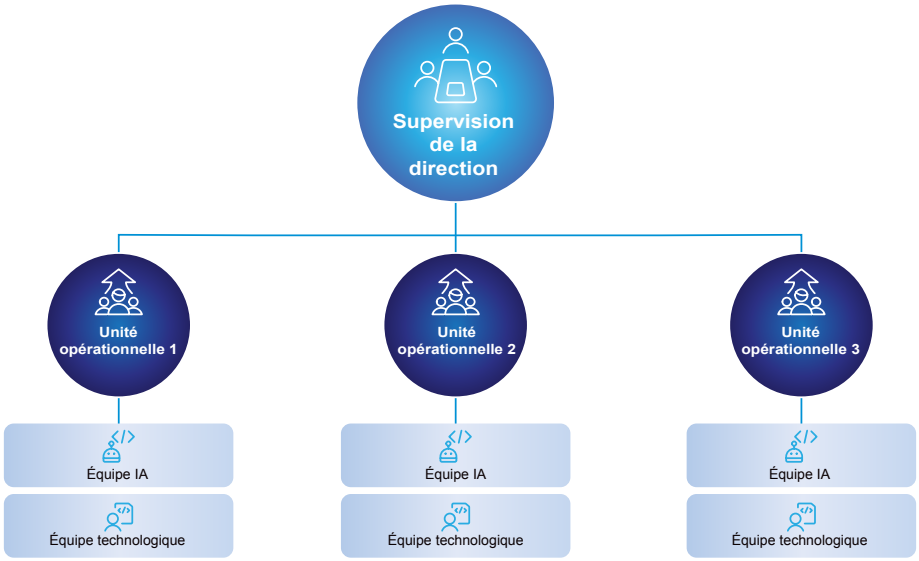


Le modèle centralisé

Le modèle Hub-And-Spoke

Dans ce modèle, un petit groupe au centre définit la stratégie et fournit des outils et des cadres, tandis que les différentes unités commerciales agissent comme des relais pour exécuter des projets dans leur domaine. Ce modèle est intrinsèquement plus agile et plus attractif pour les entreprises qui possèdent des compétences technologiques dans d'autres unités commerciales. Il est également plus agile et évolutif pour permettre à l'entreprise de mener plusieurs projets en parallèle. L'un des points litigieux de ce modèle est la question de savoir qui possède, forme et peaufine le MLE. En général, cela appartient au hub, et les unités commerciales sont responsables des applications d'IA agentique.

Le modèle Hub-And-Spoke



Le modèle fédéré

Le modèle fédéré

Dans ce modèle, il n'existe pas de fonction centralisée et chaque unité commerciale dispose d'un groupe chargé d'exploiter ses propres systèmes et technologies d'IA. Dans certains cas, une petite équipe peut assurer la supervision de l'entreprise. En général, ce modèle offre un contrôle complet aux unités commerciales, ce qui leur permet d'accélérer la mise en œuvre ; toutefois, cela se fait au détriment de la gouvernance et des risques de sécurité. Ce modèle serait particulièrement utile pour les organisations extrêmement matures.

Modèle hybride

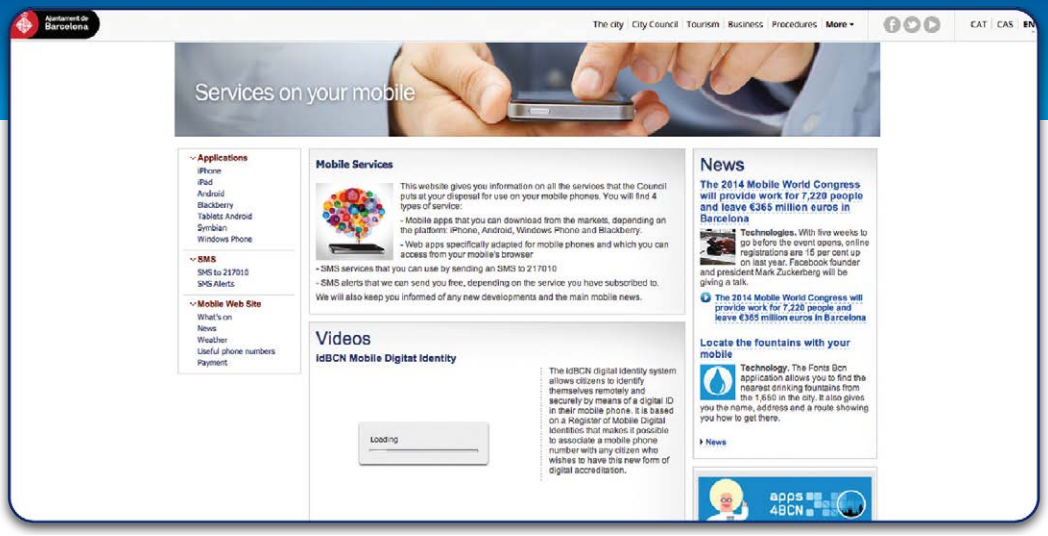
Les modèles hybrides combinent des composants issus des autres approches. Le principal avantage réside dans la possibilité de tirer parti des économies d'échelle en proposant des services standard que les équipes peuvent utiliser, tout en donnant aux unités commerciales l'autonomie nécessaire pour les fournir.

En fin de compte, le choix du bon modèle dépend des besoins spécifiques de l'entreprise. Pour réussir, vous devez comprendre comment vous souhaitez que vos équipes travaillent et quelles mesures de protection vous souhaitez mettre en place pour vos utilisateurs. Cette clarté est essentielle pour développer des applications d'IA agentique évolutives, axées sur les résultats et dotées d'une capacité d'action.

Dans l'étude de cas suivante, la ville de Barcelone a mis en œuvre un modèle Hub-and-Spoke pour mettre les données et les services à la disposition de tous les citoyens depuis n'importe quel appareil et n'importe où, améliorant ainsi l'accès aux services et la qualité de vie globale de ses citoyens.

Étude de cas

Ville de Barcelone



La ville de Barcelone : les services aux citoyens sont « à portée de main »

La ville de Barcelone est la deuxième plus grande ville d'Espagne, avec plus d'un million et demi d'habitants. Pour réaliser sa vision de transformation en une ville intelligente, le gouvernement municipal s'appuie sur des solutions d'administration en ligne mobiles et basées sur le cloud pour faciliter l'engagement des citoyens dans les processus administratifs et les services de la ville.

Les objectifs de la mise en œuvre d'un système d'administration en ligne sont clairs : mettre les données et les services à la disposition de tous les citoyens, depuis n'importe quel appareil et n'importe où, afin d'améliorer la qualité de vie de tous. La première étape pour y parvenir a été de rendre les données du conseil municipal et d'autres données disponibles en format numérique, tout en promouvant la réutilisation de ces informations pour stimuler la croissance économique grâce à des opportunités d'innovation.

Pour normaliser ses informations, la Ville devait consolider son infrastructure sur la base de normes ouvertes et interopérables et mettre hors service ses anciens systèmes. La Ville a choisi de migrer ses solutions vers le cloud. Un système de gestion de contenu hébergé dans le cloud constitue une alternative fiable, flexible et génératrice de gains économiques à long terme. Le résultat a été le premier site de données ouvertes de Barcelone avec 510 ensembles de données. La solution, basée sur les principes de mobilité, de villes intelligentes et d'administration, de systèmes d'information et d'innovation, prend en charge 150 portails avec plus de 4 millions de visites d'utilisateurs et plus de 65 millions de pages générées chaque mois.

Votre entreprise est-elle prête ?

L'engouement pour l'IA a déclenché une course à l'adoption, motivée par la peur d'être distancé. Mais les entreprises véritablement innovantes n'ont pas appuyé sur l'accélérateur : elles ont freiné. Elles ont compris que si les données constituent le carburant du moteur de l'IA, les exploiter sans orientation ne vous mène pas plus loin – cela risque seulement de les épuiser avant que vous n'atteigniez votre destination.

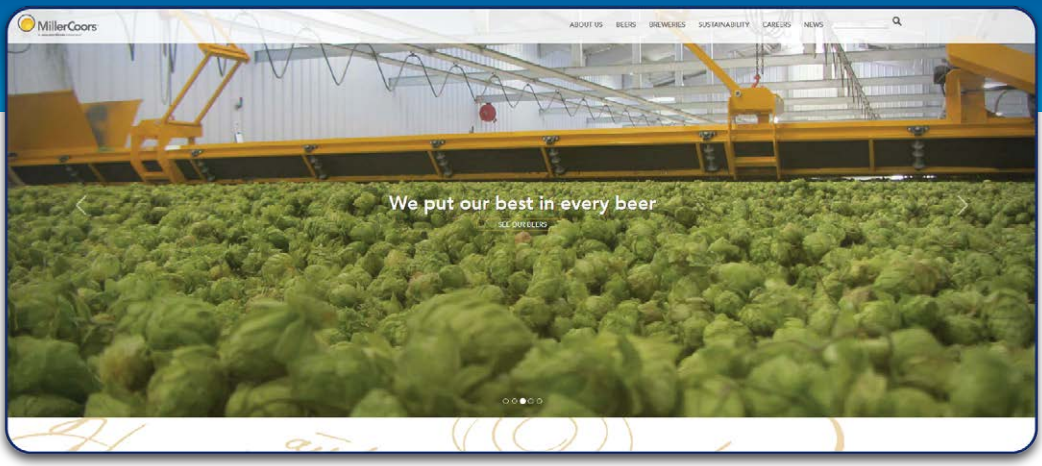
Les entreprises qui ont mis du temps à apprendre, à planifier et à se préparer ont obtenu de bien meilleurs résultats. En s'assurant que leurs données étaient prêtes et que la gouvernance était en place, ils savaient comment ils utiliseraient l'IA avant d'accélérer, une étape cruciale manquée par ceux qui ont accéléré dès le départ.

Même Microsoft a ralenti le rythme lors du déploiement de Copilot au cœur de son entreprise. En tant que l'une des premières entreprises à déployer à grande échelle, elle a divisé sa mise en œuvre en plusieurs phases distinctes, allant d'un déploiement en accès anticipé limité pour des groupes spécifiques à des groupes plus ciblés, pour finalement un déploiement complet par cohorte. Ils ont déclaré : « Nous avons divisé notre adoption selon deux vecteurs : les organisations internes telles que le service juridique ou les ventes et le marketing, et les régions comme l'Amérique du Nord ou l'Europe. Les différentes cohortes ont des objectifs différents, mais la stratégie est similaire. » [62] Cette approche spécifique par cohorte a été citée par d'autres entreprises comme la clé du succès de leur déploiement de l'IA, car ils cherchaient à fournir à des groupes et à des utilisateurs spécifiques une technologie adaptée à leurs besoins, favorisant ainsi l'adoption.

MillerCoors agit en tant que point focal ou plaque tournante de sa chaîne d'approvisionnement en supervisant directement ses fournisseurs dans l'étude de cas suivante.

Étude de cas

Miller Coors



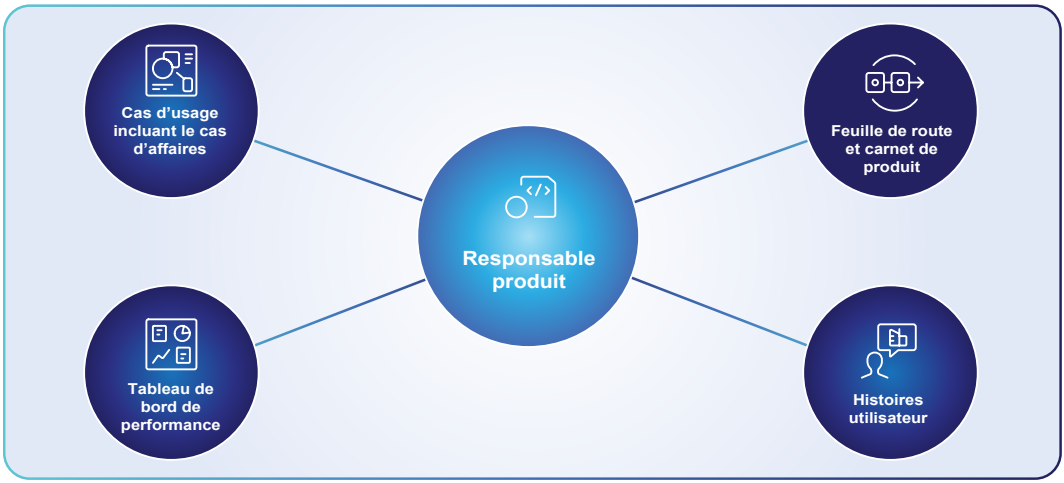
Miller Coors

MillerCoors est une coentreprise des activités américaines de SABMiller et Molson Coors. Avec plus de 450 ans d'expérience brassicole combinée, MillerCoors possède un portefeuille impressionnant de bières de pointe. Avec près de 30 % des ventes de bière aux États-Unis, MillerCoors est la deuxième plus grande entreprise brassicole des États-Unis. L'entreprise exploite huit grandes brasseries, ainsi que plusieurs brasseries artisanales.

Miller Brewing (une ancienne société de MillerCoors) a constaté que sa chaîne d'approvisionnement du distributeur au détail ne répondait pas aux normes du secteur et, surtout, aux attentes des utilisateurs. L'entreprise avait besoin de moderniser et de standardiser ses processus inefficaces et gourmands en documents pour rester compétitive sur son marché complexe et centré sur le consommateur.

À l'aide de services gérés B2B, Miller Brewing a connecté plus de 400 distributeurs à 25 systèmes commerciaux différents au sein d'une plateforme EDI (échange de données informatisé) cohérente. Cela a permis à l'ensemble de leur réseau de distributeurs de faire affaire avec n'importe quel détaillant ayant besoin d'une capacité EDI.

Les services gérés B2B fournissent la base technique d'une plateforme EDI transparente de bout en bout pour toutes les connexions fournisseurs et bancaires de MillerCoors. Les documents critiques sont reçus, traités et échangés de manière transparente afin d'améliorer l'efficacité, de réduire les coûts et, bien sûr, de garantir la livraison de la bière. En un an seulement, la transformation de l'entreprise a éliminé 1,2 million d'heures de travail pour les distributeurs et 1,3 million d'heures pour les détaillants, pour un total de 2,5 millions d'heures de travail supprimées de la chaîne d'approvisionnement du distributeur au détaillant. Les économies de temps se traduisent par une réaffectation estimée de 1 200 ressources en équivalent temps plein (ETP) à d'autres tâches, ce qui pourrait permettre de réaliser des économies de main-d'œuvre de 50 millions de dollars.



Large champ d'action du propriétaire du produit

2. Développement d'applications IAE agentique

Commencez petit, restez simple

Au-delà d'une approche de déploiement spécifique à une cohorte, l'un des principes fondamentaux d'une mise en œuvre réussie de l'IA est de commencer modestement et de rester simple. Ceci repose sur une attention rigoureuse portée à l'obtention de résultats commerciaux. La technologie au service de la technologie est un concept intéressant qui peut certainement être amusant pour les équipes technologiques, mais ce n'est pas une stratégie gagnante avec l'IA.

Commencer modestement signifie choisir un cas d'utilisation et travailler avec une entité de votre entreprise qui comprend la technologie et son potentiel, qui dispose de bons processus métier documentés, de données de bonne qualité et qui peut favoriser son adoption. Il ne faut pas sous-estimer l'impact culturel des agents du changement et des prescripteurs, qui peuvent favoriser l'adoption. Dans notre cas, il s'agissait de sélectionner notre équipe des ressources humaines. Grâce à une forte orientation technologique au sein de cette équipe, ils étaient désireux d'embrasser la transformation et de jouer leur rôle à la fois en tant que propriétaire d'entreprise et de chef de produit. *

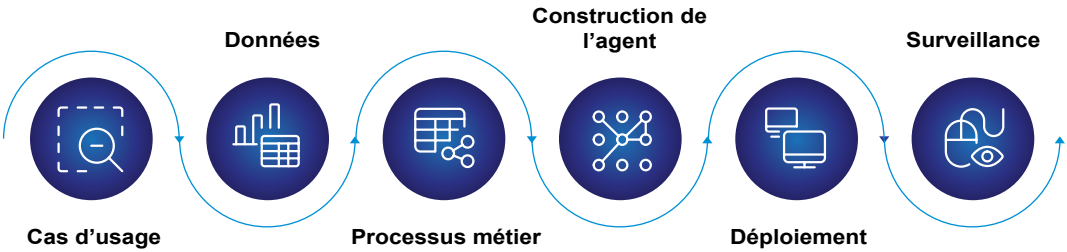
Les propriétaires de produit jouent un rôle essentiel dans la conception et la mise en œuvre de cas d'utilisation spécifiques de l'IA. S'assurer qu'ils peuvent agir en tant qu'agents du changement et prescripteurs de l'adoption de l'IA agentique est tout aussi crucial que de s'assurer qu'ils possèdent les compétences requises pour ce rôle. La portée plus large du rôle de propriétaire du produit est illustrée ci-dessus.

* À titre de référence, le cadre SAFe (Scaled Agile Framework) définit le propriétaire du produit comme « la voix du client et de l'entreprise, gérant et hiérarchisant le backlog de l'équipe, alignant le travail de l'équipe en fonction de la stratégie et des besoins des parties prenantes, et en aidant à maintenir l'intégrité commerciale et technique de la solution. » [63]

L'importance de bons processus et de données pour piloter les applications d'IA agentique

Une fois le cas d'utilisation défini pour l'équipe et la cible, une compréhension approfondie des données et des processus métier devient essentielle pour guider le développement et le comportement de l'agent. Le processus est décrit ci-dessous.

Approche de gestion du cycle de vie pour l'IA agentique



Le cycle de vie de l'IA agentique

Sur la base du **cas d'utilisation**, le processus commence par une analyse **des données et des processus métier**. Cette analyse éclaire directement le développement de l'application d'intelligence artificielle agentique.

Cette phase de développement, souvent pilotée par le propriétaire du produit, est généralement le fruit d'une collaboration entre le service informatique et l'unité commerciale concernée. Pour réduire les obstacles à l'entrée, de nombreux environnements de développement agentiques utilisent désormais des approches low-code/no-code, permettant aux non-développeurs de contribuer.

Une fois l'**agent** créé, l'application passe en phase de **déploiement**. Cette étape nécessite une approche standardisée afin de garantir la bonne gouvernance et la mise en place de garde-fous pour l'entreprise. Enfin, le processus est complété par une **surveillance** continue pour gérer les performances.

Le succès d'un agent repose souvent sur une compréhension unifiée de son rôle, des données et des processus qu'il utilise, ainsi que de ses entrées et sorties. Au-delà de cela, il est essentiel de documenter soigneusement ses comportements attendus pour réussir. La meilleure façon d'y parvenir est de commencer modestement. Cela implique de commencer par des agents simples à fonction discrète et d'éviter les scénarios complexes comportant de nombreux cas extrêmes. À mesure que ces agents simples commencent à apporter de la valeur, des scénarios plus complexes peuvent être abordés par le biais d'une série de flux d'orchestration ou d'agents plus complexes.

3. Collaboration entre les équipes d'IA humaines et agentiques

Traiter les agents numériques comme une extension de votre personnel

Les agents numériques doivent-ils être gérés par les ressources humaines, au même titre que les employés humains ? Cette question est certainement un sujet de débat alors que les applications d'IA agentique se généralisent. Dans son rapport sur l'organisation agentique, McKinsey & Company a examiné comment les entreprises tirent parti des employés humains et des agents numériques pour obtenir des résultats :

> « Au fur et à mesure que les agents se chargent de l'exécution, les personnes définiront de plus en plus les objectifs, feront des compromis et orienteront les résultats. Cela changera la façon dont les entreprises planifient une main-d'œuvre hybride, les personnes qu'elles embauchent (ou empruntent), la manière dont elles déploient les talents humains ou issus de l'IA et la manière dont elles mesurent le succès. Les systèmes RH suivent non seulement les employés humains, mais constituent également un référentiel d'agents et de flux de traitement agentiques. » [64]

L'une des approches efficaces adoptées par certaines entreprises consiste à élaborer des descriptions de poste pour leurs agents (voir ci-dessous). Nous avons adopté cette pratique en interne, nos équipes créant des descriptions de poste au cours du processus de développement initial, similaires à celles que nous publions pour les rôles humains. Cela garantit qu'au fur et à mesure que nous entamons la phase de déploiement et de mesure, nous connaissons les attentes. Sur le plan culturel, cela a également aidé notre équipe à mieux comprendre son propre rôle par rapport à ces nouveaux agents numériques.

Description du poste humain : Spécialiste des opérations RH

Résumé des rôles
Le spécialiste des opérations RH est chargé de gérer et de résoudre les tickets RH des employés, en mettant l'accent sur la sélection des avantages, l'intégration et les directives politiques. Ce rôle fonctionne en tandem avec un assistant d'IA agentique pour garantir un soutien rapide, précis et personnalisé.

Principales responsabilités

- Passer en revue et validez les demandes de sélection d'avantages soumises par les employés.
- Fournir des conseils personnalisés en fonction de l'éligibilité, du lieu de travail et du rôle des employés.
- Transférer les cas complexes ou exceptionnels à la direction des ressources humaines.
- Collaborer avec l'agent AI pour surveiller les files d'attente de tickets et prioriser les cas urgents.
- Auditer les sélections d'avantages pour vérifier leur conformité aux politiques internes et aux exigences réglementaires.
- Entraîner et étalonner l'agent AI en passant en revue ses recommandations et ses boucles de rétroaction.

Compétences et qualifications

- Au moins 3 ans d'expérience dans le domaine des ressources humaines ou de l'administration des avantages sociaux.
- Solide compréhension des systèmes HRIS d'entreprise et des plateformes d'avantages sociaux.
- Excellentes compétences en communication et en prise de décision.
- Travaillez confortablement aux côtés de tous les agents et des flux de traitement numériques.

Collaboration avec AI Agent

- Superviser et approuver les recommandations d'avantages générées par l'agent.
- Fournr un contexte et des nuances pour les cas extrêmes que l'agent signale comme ambigus.
- Participer à l'amélioration continue des flux de traitement agentiques et des données de formation.

DDescription du poste d'agent d'IA agentique : Agent de résolution de tickets RH

Résumé du poste
L'assistant IA agentique est conçu pour traiter de manière autonome les tickets liés aux ressources humaines, en mettant principalement l'accent sur la sélection des avantages. Il fonctionne en étroite coordination avec les spécialistes des ressources humaines afin de garantir l'exactitude, la conformité et la satisfaction des employés.

Principales responsabilités

- Classer et acheminer automatiquement les tickets RH entrants en utilisant la compréhension du langage naturel.
- Récupérer et analyser les données des employés (par exemple, durée, lieu, niveau d'emploi) afin de recommander des programmes d'avantages sociaux appropriés.
- Générer des synthèses d'avantages personnalisés et des FAQ pour les employés.
- Signaler les billets nécessitant un jugement humain ou des exceptions à la politique.
- Tirer parti des commentaires humains et mettre à jour les modèles de décision en conséquence.
- Conserver les journaux d'audit et la traçabilité de toutes les actions entreprises.

Capacités

- Intégrer les systèmes SIRH, de paie et d'avantages sociaux de l'entreprise à l'aide d'APL sécurisés, vérifiables et approuvés.
- Utiliser les documents de politique et les données historiques des tickets pour prendre des décisions éclairées.
- Disponible 24 heures sur 24, 7 jours sur 7, avec des capacités de réponse en temps réel.
- S'améliorer en permanence grâce à l'étalonnage basé sur les commentaires et au réglage du modèle.

Collaboration avec l'homme

- Envoyer les recommandations relatives aux avantages au spécialiste des opérations RH pour approbation.
- Recevoir des commentaires sur les recommandations rejetées ou modifiées afin d'affiner les résultats futurs.
- Alerter l'humain en cas d'anomalies, de données manquantes ou de conflits de politiques.

Gouvernance et supervision

- Toutes les actions sont enregistrées et soumises à un examen par des agents d'audit automatisés et des équipes de spécialistes des ressources humaines.
- Le système fonctionne de manière autonome, mais sous surveillance et auditabilité continues et fait l'objet d'audits périodiques pour valider la conformité et les performances du modèle.

Étape	Assistant IA Agentique	Spécialiste Humain
1. Réception du ticket	Classe le ticket comme « Sélection des avantages » et extrait les données pertinentes de l'employé.	Surveille la file et examine les tickets signalés.
2. Recommandation	Propose un ensemble d'avantages selon les règles de la politique et le profil de l'employé.	Vérifie la recommandation pour en assurer la précision et la pertinence.
3. Communication	Envoie un résumé à l'employé avec des liens vers les formulaires d'inscription et les FAQ.	Fait un suivi avec l'employé en cas de besoin de clarification ou d'escalade.
4. Gestion des exceptions	Signale les tickets avec données manquantes ou conflits de politique.	Résout les exceptions et met à jour les données d'entraînement de l'agent.
5. Audit et rétroaction	Enregistre les actions et apprend à partir des retours humains.	Audite les décisions de l'agent et fournit des commentaires pour améliorer.

Comment l'assistant humain et l'assistant IA agentique travaillent ensemble pour sélectionner les avantages sociaux d'un employé

L'évolution de l'IA agentique ne consiste pas à remplacer les personnes par l'automatisation, mais à redéfinir la façon dont les humains et l'IA travaillent ensemble en tant que partenaires complémentaires. Dans tous les secteurs, les entreprises chefs de file redéfinissent les rôles et les flux de traitement afin d'intégrer l'IA dans les fonctions éditoriales, créatives et stratégiques. Plutôt que de considérer l'IA comme une menace, elles l'adoptent comme un catalyseur d'efficacité et d'innovation. La différence réside dans l'état d'esprit : le succès favorise les entreprises qui abordent l'adoption de l'IA avec détermination et clairvoyance, en réformant les équipes, en repensant les processus et en intégrant l'IA là où elle amplifie les capacités humaines.

À la base, cette transformation fait passer l'IA d'un point névralgique émotionnel à un avantage opérationnel. Les professionnels de la création (rédacteurs, éditeurs, concepteurs) ne sont pas remplacés ; leurs capacités sont renforcées. L'intelligence artificielle d'entreprise accélère désormais la recherche, produit les premières ébauches et automatise la production de routine, laissant ainsi le temps et l'espace nécessaires aux utilisateurs pour qu'ils puissent se concentrer sur ce qu'ils font le mieux : élaborer une stratégie, préserver l'intégrité de la marque et exercer leur jugement humain là où cela compte le plus.

Dans la fonctionnalité ci-dessous, l'IA, les agents humains et les flux de traitement existants orchestrent les flux sécurisés entre les ensembles de données publics et privés au sein d'un cloud privé, automatisant les réclamations, protégeant les informations sensibles et garantissant la conformité. Ce modèle allie l'agilité du cloud public à la gouvernance sur site et à l'intégrité des données de bout en bout.

Greffier du Circuit Court d'un comté américain

Le greffier du Circuit Court d'un comté américain supervise un écosystème judiciaire complexe : il tient à jour les dossiers judiciaires, sécurise les preuves, perçoit les amendes et gère la documentation dans 24 municipalités et zones non incorporées. Pendant des décennies, les systèmes papier ont créé des goulots d'étranglement : les greffiers vérifiaient manuellement les citations, les juges s'appuyaient sur des dossiers cartonnés et chaque étape de saisie des données ralentissait le rythme de la justice. Le défi n'était pas seulement l'inefficacité – mais son échelle. À mesure que la croissance démographique s'accélérait, le volume des affaires des incidents de circulation menaçait de surcharger le personnel et de retarder les décisions des tribunaux.

En introduisant l'automatisation pilotée par l'IA au sein d'une plateforme de gestion des affaires gouvernée, le comté a transformé le fonctionnement de ses salles d'audience. L'IA agentique surveille désormais l'état des dossiers, valide les dossiers et achemine les documents en toute sécurité entre les systèmes, tandis que les greffiers humains interviennent pour approuver les exceptions et vérifier les cas extrêmes. Les juges peuvent récupérer instantanément l'historique des affaires numériques, accéder aux bases de données intégrées sur le trafic de l'État et consulter les citations antérieures via un tableau de bord unifié.

Dans les coulisses, les agents d'intelligence artificielle connectent le système de billetterie embarqué, les référentiels de documents et les bases de données judiciaires du comté, automatisant ainsi la saisie, la classification et la validation des informations. Les données sensibles ne quittent jamais le cloud privé du comté, et chaque point de décision est enregistré à des fins d'audit et de conformité. Ce qui nécessitait autrefois la saisie manuelle des données se fait désormais en quelques secondes, ce qui permet aux employés de se concentrer sur des tâches à plus forte valeur ajoutée et de réduire le risque d'erreur humaine.

Grâce à ce modèle d'intelligence artificielle hybride, combinant automatisation agentique et supervision humaine, le bureau du greffier a modernisé l'ensemble de son écosystème d'informations. Résultat : un traitement des dossiers plus rapide, une meilleure intégrité des données et un alignement complet avec les mandats des États en matière de partage d'informations. Il s'agit d'un modèle pour une IA responsable dans le gouvernement, qui montre comment les systèmes intelligents et le jugement humain peuvent fonctionner côte à côte pour fournir un service public plus fiable et plus efficace.

4. Gestion et mesure du rendement

Mesurer le succès de votre application IA agentique

La mesure des résultats est au cœur de la réussite ou de l'échec d'une application d'IA agentique. Par conséquent, ces mesures doivent être clairement définies dès le départ dans une description de poste qui décrit l'objectif, les tâches et les paramètres de l'agent. Cette « description de poste », créée lors de l'élaboration de l'analyse de rentabilisation, est essentielle pour définir la portée appropriée du rôle de l'agent.

Aujourd'hui, il n'existe pas de norme universellement définie ou adoptée pour les KPI des applications IAE agentique, bien qu'il existe des normes dans de nombreux pays et organismes de réglementation autour de l'IA (éthique, transparence, risque, etc.). En l'absence de norme universelle, les entreprises peuvent tirer parti des nombreux environnements de développement du domaine public, soit en en adopter un directement ou en l'adaptant, en fonction de leur mise en œuvre spécifique.

Un cadre proposé dans *l'International Journal of Scientific Research and Modern Technology examinait* « cinq dimensions vitales : la qualité du modèle, la performance du système, l'impact commercial, l'interaction homme-IA et les considérations éthiques et environnementales ». En ce qui concerne la dimension de la qualité du modèle, l'article a examiné l'exactitude, la précision, l'achèvement des tâches, les hallucinations et le rendement. Les indicateurs clés de performance (KPI) opérationnels étaient axés sur la latence, le débit et l'utilisation des ressources. L'impact commercial a évalué le retour sur investissement, les économies de coûts, les améliorations de productivité et l'impact sur le marché. L'interaction homme-IA a été examinée en termes de satisfaction, de confiance, d'adoption et d'engagement des utilisateurs. Enfin, en termes de considérations éthiques et environnementales, le document a examiné les préjugés, l'équité, la transparence, l'impact environnemental et la dérive éthique. [65]

Bien que tous ces KPI ne soient pas pertinents pour tous les déploiements d'IA agentique, il est important que les équipes adoptent une approche holistique pour sélectionner les différentes dimensions. Une fois les KPI pertinents déterminés, ils peuvent être formalisés sous forme de tableau de bord. Cette approche reflète celle utilisée avec succès pour l'automatisation robotique des processus (ARP), où les tableaux de bord étaient essentiels pour favoriser l'automatisation et l'efficacité. La même rigueur doit être appliquée ici, avec des évaluations quotidiennes par rapport aux principales dimensions de l'agent.

Il est tout aussi important de disposer d'un cadre et d'un processus de remédiation définis. Toutes les applications d'IA d'entreprise ne seront pas couronnées de succès, et pour celles qui échouent, ce cadre est essentiel pour comprendre la cause première et prendre une décision basée sur les données quant à savoir s'il faut investir dans un correctif ou le mettre hors service. Ce processus soutient directement la culture de « l'échec rapide », un changement auquel de nombreuses entreprises ont du mal à faire face. Les équipes doivent apprendre à accepter qu'il vaut mieux mettre hors service un projet défaillant, plutôt que de se forcer à déployer un projet qui n'atteindra jamais les résultats escomptés.

Il est également important de se rappeler que l'IAE s'appuie sur des données contextuelles sécurisées, et pas seulement sur la quantité. En connectant les systèmes structurés, le contenu non structuré et les flux interorganisationnels à travers le cloud GIE, les entreprises peuvent former et déployer des agents qui agissent de manière responsable, suivent leurs décisions et répondent aux exigences de conformité dès la conception. Dans le chapitre suivant, nous examinerons l'évolution de l'IA agentique à l'IAG.

Télécharger The Fast Five

1. **Choisissez le bon modèle organisationnel pour le déploiement de l'IA.**
   Le choix d'un modèle de déploiement approprié (centralisé, hub-and-spoke, fédéré ou hybride) est essentiel pour une adoption réussie de l'IA agentique. Le modèle doit clarifier la propriété, la responsabilité et la gouvernance, en équilibrant le contrôle avec l'agilité en fonction des besoins de votre secteur et de l'environnement réglementaire.

2. **Adoptez une stratégie de déploiement par étapes et basée sur les cohortes.**
   L'adoption précipitée de l'IA entraîne souvent des erreurs. Les entreprises performantes déploient des applications d'IA agentique par phases délibérées ciblant des unités commerciales ou des régions spécifiques. Cette approche axée sur les cohortes garantit la préparation, maximise l'adoption par les utilisateurs et adapte le support aux besoins uniques de chaque groupe.

3. **Commencez modestement, concentrez-vous sur la valeur commerciale et bâtissez sur la réussite.**
   Commencez par des cas d'utilisation simples et bien définis, en donnant la priorité aux unités commerciales dotées de processus matures et de données de qualité élevée. Donnez aux agents du changement, tels que les chefs de produit, les moyens de favoriser l'adoption et d'itérer en fonction des premiers résultats avant de passer à des scénarios plus complexes.

4. **Intégrez les agents numériques à la planification et à la gestion des effectifs.**
   Traitez les agents d'intelligence artificielle comme une extension de votre personnel. Définissez clairement les rôles et les attentes des agents numériques, en adoptant des pratiques RH telles que les descriptions de poste et des objectifs de performance pour garantir l'alignement entre les membres humains et les membres de l'équipe d'IA, et pour favoriser la compréhension et l'acceptation au sein de l'entreprise.

5. **Mettez en œuvre des mesures de performance et des mesures correctives rigoureuses.**
   Le succès repose sur des KPI clairement définis dans de multiples dimensions (qualité du modèle, impact commercial, interaction homme-IA, éthique et performance du système). Développez des fiches de performance pour les agents, évaluez régulièrement les résultats et préparez-vous à corriger ou à supprimer les applications peu performantes. Adoptez une culture qui apprend des échecs et qui se répand rapidement.

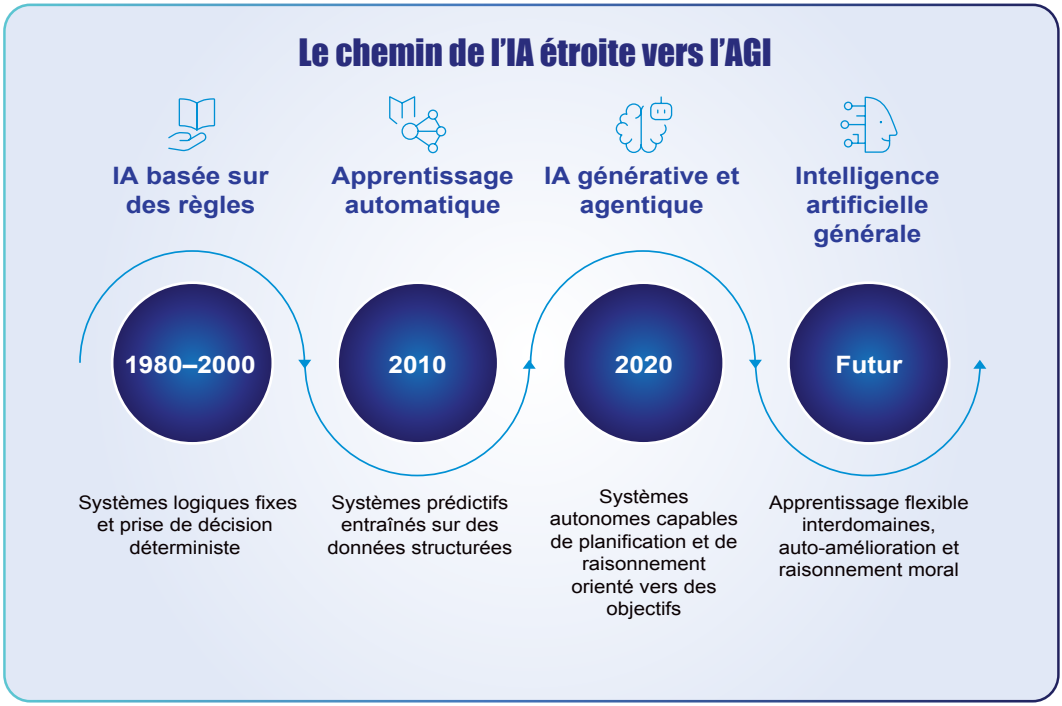
Chapitre dix

La création d'IAG à partir d'une IA agentique

Comme nous l'avons expliqué dans ce livre, l'histoire de l'IA est une histoire d'aspiration et d'innovation, c'est-à-dire le désir de créer des systèmes capables de calculer et de comprendre, de réagir et de raisonner. L'IA agentique nous donne un aperçu de ce qui est possible et nous oriente vers les modèles frontière qui ouvrent la voie à l'intelligence générale artificielle (IAG). L'IAG étendra la trajectoire de l'IAE vers des systèmes capables de généraliser à la manière humaine, d'apprendre dans différents domaines, de former des concepts abstraits et d'agir de manière autonome.

Les entreprises qui souhaitent déployer des systèmes intelligents à grande échelle doivent planifier la gouvernance, l'orchestration et la gestion du cycle de vie des réseaux d'agents, et pas seulement des modèles individuels. Au fur et à mesure que ces cadres évoluent, ils servent de base pour passer de l'IA agentique à des systèmes cognitifs plus larges et plus adaptatifs, des systèmes qui remettront en question les modèles architecturaux, opérationnels et de gouvernance traditionnels.

Ce chapitre explore le passage de l'IA agentique (systèmes qui poursuivent des objectifs et apprennent sous la supervision humaine) vers la promesse de l'AGI, une forme d'intelligence capable de comprendre, de raisonner et de s'adapter comme un être humain dans divers contextes. Il met en lumière les fondements techniques et éthiques nécessaires à cette transition et explore le débat en cours sur la question de savoir si l'IAG découlera de l'extension des modèles actuels ou des avancées dans les nouvelles architectures, les capacités de raisonnement et l'intelligence émotionnelle.



Le chemin de l'IA étroite à l'IAG

L'IA agentique : Le pont vers l'IAG

Bien que l'IA agentique puisse effectuer des actions spécifiques à des tâches, elle est soumise à des contraintes de domaine et ne peut pas apprendre d'un domaine à l'autre. Son raisonnement est contextuel mais non conceptuel ; il ne peut pas abstraire des principes ou généraliser l'apprentissage. En revanche, l'IAG peut apprendre, raisonner et s'adapter à un large éventail de tâches. L'IAG aborde l'intelligence flexible caractéristique de la cognition humaine.

La transition de l'IA agentique à l'IAG n'est pas simplement une question de plus de données, mais d'approche architecturale. Les chercheurs se demandent si l'IAG émergera de la mise à l'échelle des modèles de base actuels ou si elle nécessitera une nouvelle méthode de raisonnement, d'expérience et d'intelligence émotionnelle. Deux approches différentes dominent les premières réflexions sur ce sujet :

1. Hypothèse d'évolution : Prévoit que l'IAG émergera de l'évolution continue des grands modèles linguistiques et multimodaux d'aujourd'hui, sans nécessiter de nouveaux algorithmes. Dans Scaling Laws for Neural Language Models, les auteurs expliquent la relation entre les performances du modèle et trois facteurs : la taille du modèle, la taille du jeu de données et la capacité de calcul. « Nos résultats suggèrent fortement que les modèles plus grands continueront à être plus performants et seront également beaucoup plus efficaces en termes d'échantillonnage qu'on ne le pensait auparavant. Les grands modèles peuvent être plus importants que le big data. Dans ce contexte, une étude plus approfondie du parallélisme des modèles est justifiée. Les modèles profonds peuvent être entraînés à l'aide du pipeline, qui répartit les paramètres en profondeur entre les appareils, mais nécessite éventuellement une augmentation de la taille des lots à mesure que de plus en plus d'appareils sont utilisés. » [66]

2. Hypothèse de discontinuité : prédit que l'AGI n'émergera pas simplement en développant les MLE ou les architectures neuronales existantes, mais qu'elle nécessitera des paradigmes, architectures ou formes de cognition fondamentalement nouveaux. Certains experts soutiennent que la mise à l'échelle des réseaux neuronaux ne produira pas d'IAG parce qu'ils manquent de raisonnement structuré, de modèles causaux et de généralisation compositionnelle, qui sont des caractéristiques essentielles de la cognition humaine. Gary Marcus, par exemple, a affirmé l'importance des symboles par rapport aux réseaux neuronaux dans le développement de l'IA :

> « Les symboles [les codages internes à l'ordinateur, tels que des chaînes de bits binaires, qui représentent des idées complexes] dépassent encore de loin les réseaux neuronaux actuels dans de nombreux aspects fondamentaux du calcul. Ils sont bien mieux placés pour raisonner dans des scénarios complexes, peuvent effectuer des opérations de base telles que l'arithmétique de manière plus systématique et plus fiable, et sont mieux à même de représenter avec précision les relations entre des parties et des ensembles (essentiel à la fois pour l'interprétation du monde 3D et pour la compréhension du langage humain). Ils sont plus robustes et plus flexibles dans leur capacité à représenter et à interroger des bases de données à grande échelle. Les symboles sont également plus propices aux techniques de vérification formelles, qui sont essentielles pour certains aspects de la sécurité et omniprésentes dans la conception des microprocesseurs modernes. Abandonner ces vertus plutôt que de les exploiter dans une sorte d'architecture hybride, n'aurait aucun sens. » [67]

Selon toute vraisemblance, le cheminement de l'IA agentique vers l'AGI ne sera pas simple, mais plutôt une combinaison d'expansion des modèles et des capacités, stimulée par l'amélioration de la qualité des données, la capacité d'interprétation des modèles, la disponibilité des ressources informatiques et l'exploitation du raisonnement symbolique au-delà des réseaux neuronaux traditionnels.

Le rôle de l'IA agentique et de l'orchestration d'entreprise

À mesure que les déploiements d'IA agentique arrivent à maturité, ils constituent une première étape vers la mise en place d'approches hybrides pour le développement de l'IAG. Avec l'IA agentique, les tâches complexes au niveau humain sont naturellement décomposables et peuvent être distribuées. Des agents spécialisés peuvent être utilisés pour des fonctions telles que la planification, la recherche, le codage, la vérification, la simulation et la gestion. Les agents exécutent des fonctions discrètes et peuvent fonctionner en parallèle et collaborer, réduisant ainsi la charge cognitive et informatique de chaque modèle.

Parallèlement, les agents spécialisés peuvent être améliorés indépendamment et réutilisés dans toutes les tâches. Les agents peuvent également adopter des approches d'apprentissage distinctes, en tirant parti de l'apprentissage par renforcement pour l'optimisation, du raisonnement symbolique pour la logique ou de l'apprentissage non supervisé pour la découverte. Cette modularité permet de créer un système d'apprentissage hybride.

En combinaison avec les agents, la couche d'orchestration fournit un mécanisme de coordination central. L'orchestrateur gère la gestion des tâches en décomposant et en attribuant les tâches, en planifiant et en allouant des ressources. Il gère également la communication en acheminant le contexte entre les agents et assure une supervision en validant les résultats, en surveillant les performances et en gérant le cycle de vie du système.

Surtout, la couche d'orchestration permet également l'orchestration de l'apprentissage, permettant à l'ensemble du système agentique de s'améliorer au fil du temps sur la base d'expériences distribuées. Cependant, il est essentiel de reconnaître que l'orchestration à elle seule n'est pas synonyme de cognition ; de nombreux systèmes actuels manquent de planification à long terme, de mémoire persistante, de raisonnement et de compréhension causale basée sur des modèles. Du point de vue de la conception, l'orchestrateur doit passer d'un simple planificateur de tâches à un méta-contrôleur doté de fonctionnalités de base telles que la gestion des objectifs, l'allocation dynamique des ressources et des rôles entre les agents, les boucles d'erreur et de rétroaction réfléchies, et les pipelines d'évaluation/assurance continus. Cette approche modulaire et orchestrée constitue une base viable pour la formation de systèmes IAG hybrides

Dans l'article suivant, découvrez comment une municipalité portugaise a amélioré sa productivité et réduit ses coûts opérationnels grâce à l'automatisation pilotée par l'IA.

Étude de cas

Une municipalité portugaise

Faisant partie de l'agglomération urbaine du Grand Lisbonne, la municipalité emploie plus d'un millier de personnes. Pour les entreprises du secteur public, la gestion de la complexité croissante des opérations numériques était problématique. Les systèmes fragmentés et les flux de traitement manuels compliquaient la classification et la priorisation des demandes, le suivi des interventions ou la tenue de dossiers précis. Les données existaient, mais pas les informations. Sans supervision intégrée, les équipes étaient obligées de prendre des décisions réactives et avaient du mal à rester en conformité avec les normes réglementaires en constante évolution. Il en a résulté un manque de transparence et de responsabilité, un obstacle que les modèles modernes de gouvernance de l'IA sont spécialement conçus pour surmonter.

Pour y remédier, l'entreprise a mis en place un cadre de gestion unifié, piloté par l'IA, capable d'orchestrer les flux de travail, de classer les demandes et de prévoir la demande de service grâce à la reconnaissance de modèles. En introduisant une gouvernance structurée et une automatisation intelligente, elle a acquis une visibilité en temps réel sur les performances, l'allocation des ressources et le respect de la conformité. Au lieu de gérer manuellement les processus, l'entreprise fonctionne désormais grâce à un système d'auto-optimisation qui apprend de chaque interaction. Les composants d'IA agentique analysent en permanence les données de performance, affinent les flux de traitement et signalent les inefficiences émergentes, ouvrant ainsi la voie à une gestion adaptative des services alignée sur la stratégie de l'entreprise.

Ces développements ne se limitent pas à une amélioration opérationnelle ; ils marquent une étape vers une intelligence d'entreprise de type IAG. L'IA étant désormais intégrée à la gestion des services, le système répond non seulement aux demandes des utilisateurs, mais les anticipe en analysant le contexte, en prédisant les résultats et en coordonnant les différentes équipes. À mesure que ces systèmes agentiques évoluent, ils constituent le fondement d'une entreprise capable d'apprendre, de raisonner et de s'améliorer à grande échelle. Ce qui a commencé comme un effort de rationalisation des opérations informatiques est devenu un modèle de coexistence entre gouvernance intelligente, supervision humaine et intelligence artificielle adaptative, créant ainsi une entreprise dans laquelle l'automatisation ne remplace pas les personnes, mais leur permet de penser et d'agir avec une plus grande intelligence.

En chiffres : L'impact de la gouvernance intelligente

- **Résolution des demandes 60 % plus rapide** après le remplacement des flux de traitement manuels par une classification et une priorisation basées sur l'IA.
- **Jusqu'à 40 % de réduction des coûts d'exploitation** grâce à l'automatisation de la gestion des contrats, des actifs et des services.
- **Visibilité totale sur** les indicateurs de performance et le respect de la conformité dans tous les domaines de service.
- **50 % d'erreurs de processus en moins** grâce à la validation automatisée, aux pistes d'audit et à la détection des anomalies en temps réel.
- **Boucle d'apprentissage continu établie** : les systèmes d'intelligence artificielle agentique affinent désormais les flux de traitement de manière autonome en fonction des tendances des données et des commentaires.
- **La collaboration interfonctionnelle** s'est améliorée entre les services, remplaçant les silos par des flux de traitement transparents et adaptatifs.

Les données en tant que catalyseur de l'AGI : alimenter l'échelle cognitive

L'évolution vers l'IAG repose sur les données, dont la qualité, la diversité et la gouvernance sont les principaux facteurs. L'IA agentique s'appuie sur des données structurées et semi-structurées dans des limites opérationnelles définies. L'IAG nécessite toutefois un ensemble de données plus riche et plus représentatif capable de soutenir un raisonnement d'ordre supérieur. C'est pourquoi le besoin de données ne fait que croître à mesure que la technologie évolue.

Les données pour l'IAG doivent saisir le contexte, la causalité et l'éthique. Cela nécessite des cadres de données, des modèles de partage de données fédérés et des infrastructures de données souveraines garantissant un accès et une utilisation responsables. Les principes de l'OCDE relatifs à l'IA (2019) et la norme ISO/IEC 42001:2023 soulignent tous deux que les systèmes d'IA doivent fonctionner selon des mécanismes de gouvernance des données bien définis garantissant équité, responsabilité et traçabilité.

Les technologies améliorant la confidentialité jouent également un rôle essentiel. À mesure que l'IA se rapproche de la cognition générale, le maintien de l'éthique et de l'intégrité des données devient aussi essentiel que les indicateurs de performance.

Gouvernance et éthique : harmoniser autonomie et responsabilité

À mesure que les systèmes d'IA agentiques deviennent plus indépendants, les questions de contrôle, de responsabilité et de supervision sont essentielles, comme nous l'avons vu au chapitre 4. Cependant, le défi augmente à mesure que nous approchons de l'IAG, dont le niveau d'autonomie dépasse les capacités humaines. Les cadres éthiques pour l'IA d'entreprise se sont historiquement concentrés sur l'équité, la transparence et leur caractère explicable. Cependant, alors que les systèmes commencent à prendre des décisions complexes, il sera important de veiller à ce que les objectifs des systèmes d'IA restent cohérents avec les valeurs humaines.

Comme indiqué au chapitre 6, les efforts de gouvernance internationale convergent autour de ce défi. La loi européenne sur l'intelligence artificielle (2024) établit des catégories de risque hiérarchisées pour l'IA et impose une surveillance stricte des applications à haut risque. La recommandation de l'UNESCO sur l'éthique de l'intelligence artificielle (2021) préconise une gouvernance fondée sur les droits de l'homme, tandis que le NIST AI RMF (2023) introduit la fiabilité en tant qu'élément mesurable. Ces initiatives garantissent que les systèmes d'IA restent soumis à l'intention et à la surveillance humaines, même si leurs capacités augmentent.

D'un point de vue politique, l'IAG pourrait permettre un nouveau niveau d'autonomie, dans lequel les systèmes pourraient s'adapter ou s'auto-améliorer de manière imprévisible. C'est dans cette optique que les chercheurs en sécurité de l'IA étudient de nouvelles normes. Encore une fois, cela doit se faire parallèlement à l'évolution de la technologie afin que, une fois l'IAG prête, les normes soient également préparées.

La pertinence des systèmes de type IAG pour les entreprises

Alors que les entreprises déploient des systèmes d'intelligence artificielle agentiques de plus en plus autonomes et interconnectés, nombre d'entre elles rencontrent déjà les premiers signes d'une intelligence générale artificielle dans la pratique, mais pas en théorie. Ce que nous appelons les systèmes « de type IAG » émergent de manière organique dans les entreprises : des agents intelligents qui tirent des leçons de multiples sources de données, coordonnent les décisions entre les services et adaptent leur comportement en fonction de l'évolution des objectifs ou du contexte externe. Il ne s'agit pas d'outils isolés ; ce sont des réseaux d'intelligence qui s'auto-optimisent, affinant continuellement la façon dont le travail est effectué.

Le changement est subtil, mais profond. Alors que l'automatisation remplaçait autrefois les tâches étroites et répétitives, l'IA agentique intègre désormais le raisonnement, la planification et l'autocorrection. Une équipe des services financiers peut déployer des agents chargés d'analyser les sentiments des clients, de prévoir le taux de désabonnement et de générer de manière autonome des stratégies de fidélisation – des activités qui couvrent le marketing, les risques et la conformité dans une boucle de circulation unifiée. Dans le secteur manufacturier, les systèmes d'intelligence artificielle peuvent déjà interpréter les données des capteurs, réaffecter les ressources de la chaîne d'approvisionnement et signaler les risques liés à l'approvisionnement éthique avant l'intervention des équipes humaines. La frontière entre l'automatisation spécialisée et la cognition à l'échelle de l'entreprise s'estompe rapidement.

Cette évolution comporte d'immenses opportunités stratégiques, mais aussi des risques. Sans une gouvernance efficace, les entreprises peuvent se retrouver à gérer des systèmes qui apprennent et agissent au-delà de leur conception initiale. Comme le note Gartner, plus de 80 % des entreprises qui utilisent l'IA à grande échelle citent la gouvernance et la transparence comme leurs principaux obstacles à l'adoption. [68]

La gestion des systèmes de type IAG nécessite de nouveaux modèles de responsabilisation et de surveillance. La gestion informatique traditionnelle a été conçue pour des systèmes statiques alors que les écosystèmes d'intelligence modernes exigent une gouvernance adaptative, dans laquelle les mécanismes de supervision évoluent parallèlement à l'IA elle-même. Le caractère explicable., l'auditabilité et les boucles de rétroaction doivent devenir des caractéristiques de conception, et non des considérations secondaires. Et alors que ces systèmes commencent à raisonner dans différents domaines, le jugement humain doit rester inchangé, non pas pour ralentir les décisions, mais pour les orienter.

En ce sens, l'IAG n'est pas un horizon lointain mais une réalité d'entreprise en pleine croissance. Les entreprises qui seront à la pointe de cette ère sont celles qui considèrent le renseignement comme une infrastructure, un élément devant être gouverné, intégré et continuellement amélioré, au même titre que les données ou la cybersécurité. Le résultat n'est pas des machines qui remplacent les capacités humaines, mais des systèmes intelligents qui les amplifient, en développant les connaissances de l'entreprise, en accélérant la transformation et en établissant une base de confiance pour l'avenir.

Dans l'article ci-dessous, une université sud-africaine de premier plan utilise un centre de services automatisé alimenté par l'IA pour transformer l'expérience des étudiants et garantir la continuité des activités en cas de crise.

Étude de cas

Une université sud-africaine

> *La valeur de l'apprentissage automatique est phénoménale pour notre communauté étudiante, comme en témoigne l'utilisation généralisée de nos agents virtuels et de nos articles de connaissances. Sans l'apprentissage automatique et l'intelligence artificielle, nous ne pourrions absolument pas aider nos utilisateurs finaux avec le peu d'agents dédiés dont nous disposons.*

Responsable du changement et de la configuration, université d'Afrique du Sud

L'une des meilleures universités d'Afrique mène des recherches pour trouver des solutions à des problèmes urgents. L'université enseigne en classe, en ligne et au sein des communautés. Confrontée à une ampleur et à une inégalité numérique sans précédent, l'université a décidé de transformer la façon dont elle dispensait l'enseignement et le soutien dans un monde de plus en plus hybride. Avec une population étudiante dépassant les 130 000 personnes et seulement quelques agents d'assistance dédiés, les processus manuels n'étaient plus viables. L'accès limité aux appareils et à la connectivité a aggravé la fracture numérique, tandis que les services non techniques ont eu du mal à s'adapter aux flux de traitement à distance. Le défi n'était pas simplement technologique, il était structurel. L'établissement avait besoin d'un modèle opérationnel intelligent capable de soutenir la continuité académique et administrative, tout en permettant à chaque étudiant de participer pleinement à un écosystème connecté.

Pour relever ce défi, l'université a repensé son cadre de services numériques autour de l'automatisation, de la gouvernance et de l'intelligence. Des systèmes pilotés par l'IA ont été introduits pour classer les demandes, prévoir la demande et acheminer automatiquement les tâches, permettant à une petite équipe de gérer d'énormes volumes d'interactions d'assistance en temps réel. Lorsque la COVID a frappé, les capacités d'apprentissage automatique ont accéléré l'adaptation dans le cadre de la transition mondiale vers l'enseignement à distance, en automatisant l'accès aux VPN, en fournissant des ordinateurs portables et en optimisant le support de connectivité pour des milliers d'étudiants. L'IA agentique est devenue l'épine dorsale invisible de l'infrastructure numérique de l'université, orchestrant les flux de traitement entre les départements et étendant l'intelligence à des fonctions non informatiques telles que les inscriptions, les services aux étudiants et les opérations de bibliothèque. Chaque système a tiré des leçons des interactions, améliorant ainsi la précision, la réactivité et l'équité au sein de l'institution.

Ce qui a commencé comme une réponse à une crise s'est transformé en un modèle d'enseignement adapté à l'IAG, un modèle dans lequel l'intelligence adaptative améliore à la fois l'échelle et l'équité. Aujourd'hui, le volume des demandes de service a augmenté de façon spectaculaire, mais l'efficacité et la transparence se sont améliorées dans une égale mesure. L'IA ne se contente pas de soutenir le personnel et les étudiants, elle collabore avec eux – en s'appuyant sur les modèles, le contexte et les commentaires pour anticiper les besoins et rationaliser la prise de décision. La transformation de l'université montre comment la gouvernance intelligente et l'automatisation agentique peuvent relier les capacités humaines et numériques, jetant ainsi les bases d'un écosystème universitaire où le renseignement est distribué, collaboratif et s'améliore continuellement.

Définir l'avenir de l'IAG : Au-delà de l'horizon technique

La poursuite de l'IAG est autant un voyage philosophique et social que technique. Alors que certains y voient le résultat logique de la mise à l'échelle des architectures actuelles (Scaling Hypothesis), d'autres y voient une redéfinition de l'intelligence elle-même, une étape vers des systèmes dotés d'intentionnalité, de raisonnement moral et de conscience de soi (hypothèse de discontinuité).

Si l'IA agentique représente l'automatisation de l'action, l'IAG représente l'automatisation de la compréhension. Les futurs systèmes d'IA doivent non seulement penser et apprendre, mais également s'aligner sur les valeurs humaines collectives, ce qui constitue un défi qui définira la prochaine décennie en matière de politique et d'innovation en matière d'IA dans les entreprises. La transition de l'IA agentique à l'intelligence artificielle ne concerne pas uniquement le fait que les machines surpassent les capacités humaines ; il s'agit également de la manière dont l'intelligence humaine et l'intelligence artificielle évoluent ensemble.

À mesure que les systèmes d'IA deviendront plus performants, ils redéfiniront également les rôles de la main-d'œuvre humaine. C'est pourquoi la supervision humaine doit rester une priorité, tant du point de vue des politiques et de la gouvernance que du point de vue de l'exécution et des opérations. Des rôles courants aujourd'hui ne seront peut-être plus nécessaires, mais de nouveaux rôles apparaîtront également. Il peut s'agir de la formation et de la gestion des capacités de l'IA agentique, de la garantie de la qualité et de la gouvernance des données, ou de l'utilisation de l'IA pour créer de nouveaux produits et capacités qui ne sont pas envisagés aujourd'hui. Chaque évolution technologique s'accompagne de nouvelles opportunités, et IAG ne fera pas exception à la règle.

L'avenir du travail ne sera pas défini par le remplacement humain, mais par le partenariat homme-machine. La conception de modèles de collaboration efficaces entre des spécialistes humains et des systèmes d'IA généralistes implique de définir clairement les rôles, l'autorité et les responsabilités dans le cadre de flux de traitement partagés. Cela implique également d'investir dans la formation continue et la maîtrise du numérique afin que les équipes comprennent comment remettre en question, interpréter et orienter les résultats de l'IA de manière responsable. Dans un monde où l'IA peut apprendre plus rapidement que ses créateurs, il est essentiel de maintenir la confiance et la surveillance éthique afin de garantir que l'intelligence serve les objectifs de l'humanité, et non l'inverse.

Dans ce chapitre, nous avons exploré l'évolution de l'IA agentique vers la possibilité de l'IAG, qui démontrerait un raisonnement, un apprentissage et une adaptabilité semblables à ceux de l'homme dans divers contextes. Cette transition impliquera non seulement de dimensionner les données, mais également d'intégrer une meilleure qualité des données, une meilleure capacité d'interprétation des modèles et un raisonnement symbolique, ouvrant ainsi la voie à des systèmes IAE hybrides capables de traiter des tâches complexes grâce à la spécialisation et à la collaboration.

À l'avenir, et étant donné que l'IAG ne remplacera pas l'intelligence humaine, mais son prochain grand amplificateur, les données gérées et gouvernées par une GIE joueront un rôle crucial en tant que facilitateur de l'IAG. Elles fourniront les connaissances de base nécessaires à ces systèmes avancés pour apprendre, prendre des décisions éclairées et s'adapter dans des environnements de plus en plus complexes et dynamiques. Les investissements réalisés aujourd'hui dans l'IA agentique seront précieux dans le cadre de l'évolution vers l'IAG.

Dans l'article suivant, découvrez comment un fournisseur d'analyse du commerce de détail mexicain transforme les données de vente en informations exploitables pour augmenter ses revenus.

Étude de cas

Une société mexicaine d'analyse du commerce de détail

> *Grâce à l'IA, nous avons réalisé un bond en avant en termes de performances et réduit considérablement les temps de réponse aux requêtes. Nos clients ont désormais à portée de main les données critiques dont ils ont besoin pour optimiser leur chiffre d'affaires.*

Directeur général, société d'analyse du commerce de détail

L'entreprise fournit une plateforme d'analyse basée sur l'IA qui permet aux détaillants d'optimiser les performances commerciales et la prise de décision. Au service de plus de 130 grandes marques de consommation en Amérique latine, le système basé sur le cloud unifie les données de vente et d'inventaire, analyse le comportement d'achat en temps réel et génère des informations prédictives pour guider des décisions opérationnelles plus intelligentes et plus rapides.

L'entreprise a décidé de résoudre l'un des défis les plus persistants du commerce : équilibrer l'offre et la demande avec précision. Dans un monde où les préférences des consommateurs changent de minute en minute, la capacité de synchroniser les décisions relatives aux ventes, aux stocks et aux prix est essentielle. Pourtant, les systèmes existants basés sur des bases de données traditionnelles avaient du mal à s'adapter au volume et à la rapidité des données générées. À mesure que le nombre de transactions augmentait, l'entreprise a constaté que son architecture était mise à rude épreuve : les requêtes étaient ralenties, les informations manquaient et la capacité à effectuer des ajustements en temps réel s'estompait. Pour les entreprises qui dépendaient de renseignements fournis en temps opportun, cela représentait bien plus qu'un obstacle technique ; il s'agissait d'un risque existentiel pour leur compétitivité.

Pour aller au-delà de la création réactive de rapports, l'entreprise a repensé sa plateforme d'analyse sous l'angle de l'IA. L'apprentissage automatique et les algorithmes adaptatifs traitent désormais des milliards de fichiers par jour, identifient les modèles de demande émergents et optimisent la distribution à grande échelle. L'introduction d'outils de simulation basés sur l'IA a permis d'exécuter en quelques secondes des stratégies de tarification prédictive qui prenaient autrefois des heures à calculer. Ces systèmes apprennent en permanence à partir des données historiques, testent de nouvelles variables et affinent les modèles d'élasticité pour des milliers de produits et de régions. Le résultat est une plateforme qui ne se contente pas de décrire ce qui s'est passé – elle anticipe ce qui va se passer ensuite, transformant l'analyse statique en un système intelligent vivant et apprenant.

Cette évolution marque le passage de l'analytique à la cognition, une étape vers l'IAG au niveau de l'entreprise. En intégrant le raisonnement, la prédiction et l'auto-optimisation dans ses opérations, l'entreprise a construit un système nerveux numérique capable de s'adapter en temps réel au comportement du marché. Chaque nouvelle transaction devient un signal d'apprentissage, renforçant les boucles de rétroaction qui orientent la stratégie future. À chaque itération, le système s'adapte de plus en plus à la prise de décision humaine, en l'amplifiant au lieu de la remplacer. Ce qui a commencé comme une recherche d'informations plus rapides s'est transformé en un aperçu de l'entreprise cognitive : une entreprise dans laquelle l'intelligence est distribuée, collaborative et en perpétuelle amélioration.

Télécharger The Fast Five

1. **L'IA agentique en tant que fondation de l'entreprise.**
   L'IA agentique constitue un tremplin crucial vers l'IAG en permettant la décomposition des tâches, la spécialisation et la collaboration entre agents autonomes. Cette approche modulaire jette les bases de systèmes de renseignement plus flexibles, évolutifs et de type humain.

2. **Des chemins concurrents vers l'IAG.**
   La transition vers l'IAG repose sur deux hypothèses dominantes : l'hypothèse de mise à l'échelle (l'IAG émerge de la mise à l'échelle des modèles actuels) et l'hypothèse de discontinuité (l'IAG nécessite des architectures et un raisonnement fondamentalement nouveaux). Les dirigeants doivent surveiller les deux trajectoires à des fins de planification stratégique et d'investissement.

3. **La stratégie en matière de données est essentielle.**
   Les progrès vers l'IAG dépendront de la qualité, de la diversité et de la gouvernance des données. Les entreprises doivent donner la priorité à des cadres de données robustes, à des technologies améliorant la confidentialité et à la conformité aux normes internationales en constante évolution afin de renforcer les capacités avancées de l'IA.

4. **Gouvernance et éthique au cœur de nos préoccupations.**
   À mesure que les systèmes d'IA deviennent plus autonomes, il est essentiel d'aligner leurs actions sur les valeurs humaines. Les dirigeants doivent défendre des cadres de gouvernance, de surveillance éthique et de gestion des risques solides afin d'anticiper les exigences réglementaires et les attentes de la société.

5. **Préparez-vous aux changements de main-d'œuvre et de politique.**
   L'évolution de l'IA agentique vers l'IAG redéfinira les rôles du personnel et les paysages politiques. L'investissement proactif dans les talents, la gestion du changement et la supervision humaine continue seront essentiels pour exploiter le potentiel d'IAG tout en atténuant les risques.

Chapitre onze

L'avenir de l'IAE et de la gestion des opérations

Souvent négligée, la gestion des opérations joue un rôle essentiel au sein de l'entreprise en soutenant toutes les unités commerciales et en stimulant la croissance de l'entreprise. Les pratiques opérationnelles ayant évolué au fil du temps, l'IA est devenue essentielle dans ce domaine. Dans ce chapitre, nous explorerons l'évolution de l'IA d'entreprise et de la gestion des opérations, et nous verrons en quoi il est essentiel de les comprendre pour maximiser les avantages des déploiements d'IA agentique.

Précédemment, nous avons examiné la convergence des données fiables et de l'IA dans la fourniture d'expériences innovantes et l'opérationnalisation de l'IA agentique. Nous avons également pris en compte ses effets sur le personnel et au sein de l'entreprise, ainsi que les stratégies de gestion et de maintien d'une main-d'œuvre basée sur l'IA.

Des descriptions de poste claires et spécifiques et des indicateurs de performance clés mesurables pour les effectifs humains et numériques sont essentiels au succès. En attribuant à la main-d'œuvre numérique une logique simple et des tâches modestes et bien définies, on lui permet de fonctionner efficacement. Lorsque plusieurs agents numériques travaillent ensemble, ils peuvent gérer des tâches plus complexes. Dans le même temps, les humains conservent le contrôle, ce qui leur permet d'identifier et de résoudre rapidement les problèmes ou les anomalies. Cette approche s'apparente à la direction d'un orchestre : lorsque chaque instrument joue son rôle, le chef d'orchestre peut facilement détecter s'il est désaccordé, garantissant ainsi une performance harmonieuse.

Les pages qui suivent se concentrent sur tous les aspects de la gestion des opérations basée sur l'IAE, essentiellement sur la manière de maintenir votre infrastructure, vos plateformes, vos données, votre personnel humain et, désormais, vos agents numériques, en harmonie 24 heures sur 24, 7 jours sur 7.

Découvrez comment un leader mondial des technologies de santé a pu améliorer ses opérations en mettant en œuvre une plateforme de maintenance prédictive automatisée sophistiquée qui tire parti d'algorithmes avancés d'intelligence artificielle et d'apprentissage automatique.

Étude de cas

Un leader mondial dans le domaine de la santé

> *Notre système de maintenance prédictive, basé sur de grandes quantités de données et des modèles d'IA avancés, nous permet de détecter et de résoudre les problèmes potentiels avant qu'ils n'aient un impact sur les opérations cliniques. Cela améliore la fiabilité de notre équipement et améliore les résultats et la satisfaction des patients.*
>
> Architecte principal, Service

Une entreprise spécialisée dans les technologies de la santé était confrontée à des défis croissants pour maintenir ses systèmes d'imagerie médicale avancés, à savoir les IRM et les tomodensitomètres essentiels au diagnostic et aux soins des patients. Une seule unité d'IRM peut enregistrer plus d'un million d'événements et produire 200 000 mesures par capteur par jour, couvrant des dizaines de milliers de points de données. Pourtant, dans un environnement aussi complexe et étroitement réglementé, le développement et la certification des dispositifs médicaux prennent des années. Bien qu'elles génèrent de grandes quantités de données opérationnelles, celles-ci n'ont jamais été structurées de manière à permettre une maintenance prédictive.

La transition a été non seulement technique, mais également opérationnelle, car l'entreprise a dû repenser les processus existants. Cela a nécessité l'intégration d'ensembles de données massifs provenant d'appareils médicaux, d'analyses avancées et de modèles d'apprentissage automatique pour prévoir et prévenir les défaillances potentielles avant qu'elles ne perturbent les soins aux patients.

L'amélioration des soins de santé aux patients est la priorité absolue de l'entreprise. Grâce à l'IA, ils sont en mesure de traiter efficacement des ensembles de données complexes et d'identifier des modèles indiquant des problèmes imminents, ce qui leur permet de prendre des mesures préventives bien à l'avance. L'entreprise a intégré plus de 200 flux de données (journaux en temps réel, rapports d'erreurs et indicateurs de performance) dans un entrepôt de données unique contenant plus de dix ans d'histoire et 1,5 pétaoctet d'informations continuellement actualisées. Les modèles prédictifs exploitent désormais ce vaste ensemble de données pour détecter les anomalies à un stade précoce, ce qui permet une maintenance proactive et réduit de 30 % les temps d'arrêt coûteux des équipements. Ce système a permis de diagnostiquer et de résoudre à distance 50 % des cas pris en charge par le service CT, et d'atteindre un taux de résolution dès la première intervention de 84 % pour les problèmes liés aux équipements sur site, améliorant ainsi l'efficacité du service de l'entreprise et les résultats globaux en matière de soins aux patients.

Définir l'avenir de l'IAG : au-delà de l'horizon technique

L'avenir de la gestion des opérations dépendra fondamentalement de l'adoption de l'IA et de son impact transformateur sur les expériences opérationnelles. Plusieurs facteurs clés sont essentiels :

1. **Transition d'opérations réactives vers des opérations autonomes**
   La réactivité n'est plus une option dans le domaine des opérations. Les cybermenaces, ainsi que la complexité des réseaux et des technologies, nécessitent des opérations autonomes 24 heures sur 24, 7 jours sur 7, qui détectent les problèmes et agissent en conséquence avant qu'ils n'affectent les clients.

2. **Évolution de la gestion des opérations**
   Au cours des deux dernières décennies, les opérations ont subi des transformations majeures, devenant beaucoup plus efficaces grâce aux avancées en matière de collecte, de gestion et d'analyse des données.

3. **Éléments fondamentaux de l'IA dans les opérations**
   Les opérations de l'IAE dépendent de cinq éléments clés : l'utilisation des données, la formulation du renseignement, les processus de prise de décision, l'intervention humaine dans le circuit opérationnel et un cycle de rétroaction complet. Cette approche holistique permet aux équipes opérationnelles de passer efficacement des méthodologies manuelles aux méthodologies automatisées.

4. **Application de l'IA dans les opérations de réseau et de sécurité**
   L'IA agentique a le potentiel de transformer les activités de réseau et de sécurité. Plus loin dans ce chapitre, nous explorerons des cas d'utilisation pratiques qui montrent comment l'IA agentique améliore l'efficacité opérationnelle.

5. **Impacts transformationnels sur les indicateurs opérationnels**
   Les transitions décrites modifient en profondeur les indicateurs opérationnels de base tels que le temps moyen de remise en service (TMRS), les niveaux de disponibilité des services, le nombre de pannes, le nombre d'incidents et la capacité à atteindre une disponibilité Five Nines (lorsque la technologie et les services sont opérationnels 99,999 % du temps, la référence en matière d'opérations). L'adoption de l'IA apportera des changements et des avantages importants dans chacun de ces domaines.

Maintenant que nous les avons présentées, nous pouvons examiner chacune des cinq transitions en détail.

1. Des opérations réactives aux opérations autonomes

La taille et l'échelle des réseaux et des opérations de l'entreprise ont fait de la surveillance manuelle et réactive une chose du passé. Historiquement, les équipes opérationnelles réagissaient aux problèmes dès qu'ils se présentaient, ce qui a conduit à une posture opérationnelle essentiellement réactive. Cependant, ces dernières années, les responsables des opérations se sont efforcés d'améliorer les capacités de leurs équipes, en optant pour une approche plus proactive. Cela implique non seulement de comprendre les incidents potentiels, mais également d'identifier et d'atténuer ces problèmes avant qu'ils ne dégénèrent en pannes importantes. Les outils de surveillance modernes ont considérablement évolué, permettant de détecter des modifications minimes des opérations, de la latence ou des indicateurs de performance liés à des services ou à des applications spécifiques. Ces outils sont conçus pour fournir des alertes précoces en cas de problèmes potentiels. À l'instar des alarmes incendie, ces alertes permettent aux équipes d'agir avant qu'un problème mineur ne se transforme en perturbation généralisée.

Malgré ces avancées, une partie importante des pratiques opérationnelles reste très réactive. L'évolution vers des opérations autonomes marque un changement significatif dans ce paradigme. Grâce à l'intégration de l'IAE, les équipes opérationnelles peuvent acquérir une compréhension plus précise de la dynamique du système, notamment des corrélations complexes entre les diverses activités et événements qui contribuent aux incidents. Cette connaissance approfondie est essentielle non seulement pour améliorer les capacités proactives des équipes, mais également pour mettre en œuvre des mécanismes d'autoguérison au sein des activités. Ces capacités autonomes permettent aux systèmes de résoudre automatiquement certains problèmes, allégeant ainsi la charge de travail opérationnelle.

Les équipes opérationnelles peuvent ainsi se concentrer sur des tâches plus prioritaires et sur des mesures préventives essentielles pour atténuer la survenue d'incidents. L'adoption de l'IAE offre une opportunité transformatrice de redéfinir la façon dont les opérations sont gérées, en passant d'une position principalement réactive à un cadre plus stratégique et proactif, essentiel dans l'environnement opérationnel dynamique d'aujourd'hui.

2. L'évolution de la gestion des opérations

La gestion des opérations est traditionnellement associée à des équipes travaillant dans des centres opérationnels discrets, surveillant en permanence les écrans pour détecter les alertes critiques. Cependant, la réalité de la gestion des opérations a considérablement évolué. À ses débuts, les opérations reposaient largement sur la surveillance manuelle et le dépannage des événements critiques. L'introduction de l'automatisation par des scripts a représenté une avancée significative, permettant aux équipes d'automatiser des tâches spécifiques, d'améliorer la répétabilité et de réduire les erreurs humaines.

Avec l'avènement de l'intelligence artificielle et l'adoption de l'IA agentique, la gestion des opérations peut désormais tirer parti de capacités analytiques plus sophistiquées. Les outils IAE peuvent assembler et analyser efficacement de grandes quantités de données, facilitant ainsi l'analyse des causes profondes en identifiant les anomalies et en détectant les modifications des modèles de données. Ce processus permet aux opérateurs de corréler différents ensembles de données, ce qui est devenu de plus en plus essentiel pour identifier les causes profondes des problèmes. La capacité à identifier rapidement ces causes est essentielle pour minimiser les temps d'arrêt opérationnels.

En outre, l'IAE améliore l'analyse prédictive au sein des opérations. En examinant les tendances, les activités, les délais et les relations entre les divers symptômes, causes et effets, l'IA facilite la prévision des défis opérationnels et des résultats. Cela marque un changement significatif dans la façon dont la gestion des opérations est abordée aujourd'hui et suggère un avenir dans lequel la gestion des opérations sera radicalement différente.

L'évolution du paysage nécessite également des changements dans les compétences requises pour la gestion des opérations. Les développeurs ont de plus en plus tendance à rejoindre les équipes opérationnelles dans des rôles tels que ceux d'ingénieur de fiabilité des sites (IFS). Ces professionnels utilisent leur expertise technique pour traiter les incidents, identifier les causes profondes et développer des solutions à ces problèmes en temps réel, afin d'éviter que les problèmes ne se reproduisent. La combinaison d'expertise du domaine et de compétences en programmation, complétée par l'IA, est de plus en plus omniprésente dans les opérations.

Le centre des opérations d'aujourd'hui constitue également le principal terrain de formation pour appliquer l'IA d'entreprise et les technologies de pointe afin de résoudre les défis à enjeux élevés. Les entreprises qui positionnent efficacement leurs centres d'opérations en tant que pôles essentiels d'innovation et de développement des talents sont mieux équipées pour attirer, former et fidéliser les meilleurs employés. Ces centres deviennent le terrain d'essai où les futurs dirigeants perfectionnent leurs compétences en matière de développement et de résolution de problèmes, garantissant ainsi un solide vivier de talents prêts à assumer des rôles de direction au sein de l'entreprise.

Alors que la gestion des opérations continue d'évoluer, elle constitue un terrain de formation précieux pour les développeurs seniors des entreprises de produits et de technologies. Ces personnes acquièrent une expérience directe des incidents affectant les clients et les activités, ce qui leur permet d'appliquer ces connaissances à des rôles de développement de produits. En fin de compte, cette compréhension de la gestion avancée des opérations éclairera de manière significative leurs futures contributions sur le terrain.

Les opérations, autrefois considérées comme une fonction désuète fonctionnant 24 heures sur 24 et uniquement axée sur les problèmes de surveillance, sont devenues le système nerveux central de l'entreprise, un véritable centre d'excellence en matière d'innovation.

C'est exactement ce que fait un détaillant sud-africain, en analysant des données sur la manière dont ses équipes utilisent l'IA pour adapter au mieux ses processus et optimiser les performances.

Étude de cas

Premier détaillant de biens de consommation en Afrique

> *Grâce à l'intégration de l'IA dans nos processus de test de produits, il ne nous faut littéralement que deux secondes pour comprendre où nous en sommes par sprint, par version, par fonctionnalité, pour chaque application que nous testons dans notre espace omnicanal.*

Responsable SQA

Avec des milliers de magasins en Afrique du Sud et dans sept autres pays, ce détaillant de biens de consommation de premier plan en Afrique gère un vaste portefeuille d'applications numériques omnicanaux. L'entreprise est également très présente dans le domaine des achats en ligne pour ses activités d'épicerie, de maison et de vêtements, notamment grâce à une application mobile pour la livraison locale ultrarapide de produits d'épicerie.

Le réapprovisionnement des magasins physiques et le bon fonctionnement des applications numériques sont essentiels sur un marché hautement concurrentiel. Sous la pression constante des délais de mise sur le marché, le détaillant a intégré l'IA dans son processus pour accélérer les tests et la mise sur le marché des produits. L'accélération de la création de scénarios de test grâce à l'IA a permis au détaillant d'adopter l'automatisation au sprint et en cours de publication. Cela leur a permis d'automatiser beaucoup plus tôt au cours de leurs sprints de deux semaines, ce qui a entraîné une augmentation massive de la couverture d'automatisation d'environ 65 % à environ 95 %.

En seulement huit semaines, sur près de vingt applications testées en omnicanal, le revendeur a réalisé quatre à cinq versions par semaine. Ils ont réduit les temps de cycle de 43 %, multiplié par 60 la fréquence des lancements et amélioré la couverture des tests grâce à des informations plus rapides, ce qui permet d'accélérer la mise sur le marché. Avec de tels résultats de performance, le détaillant étudie la possibilité d'appliquer l'IA à d'autres fonctions commerciales.

3. Composantes essentielles des opérations pilotées par l'IA

Au fur et à mesure que les entreprises font évoluer leurs opérations et adoptent des capacités d'IA avancées, plusieurs couches fondamentales doivent être abordées.

A. La couche de données

Il est essentiel de créer une couche de données unifiée et accessible. Les opérations traditionnelles souffraient souvent de données fragmentées, réparties entre plusieurs systèmes, outils de gestion des services et silos organisationnels. Le fait de rassembler ces ensembles de données et de permettre aux agents d'intelligence artificielle d'opérer sur eux améliore considérablement la visibilité et les capacités de détection. Par exemple, l'intégration de la sécurité et des opérations réseau permet d'analyser les journaux de sécurité en même temps que les données du réseau. Cet ensemble de données élargi permet aux équipes d'identifier et de résoudre les problèmes ou les incidents plus efficacement en ayant une vue d'ensemble en temps réel.

B. La couche de renseignement

C'est là que les modèles linguistiques, l'apprentissage automatique et les plateformes d'intelligence artificielle générative et agentique fonctionnent. Au sein de cette couche, des corrélations sont établies, des connaissances sont acquises et les applications d'IA commencent à fonctionner aux côtés d'analystes humains. L'IA générative améliore la compréhension de la situation et permet des réponses plus rapides et mieux informées au sein du centre des opérations. Les applications d'IA agentique permettent des opérations autonomes.

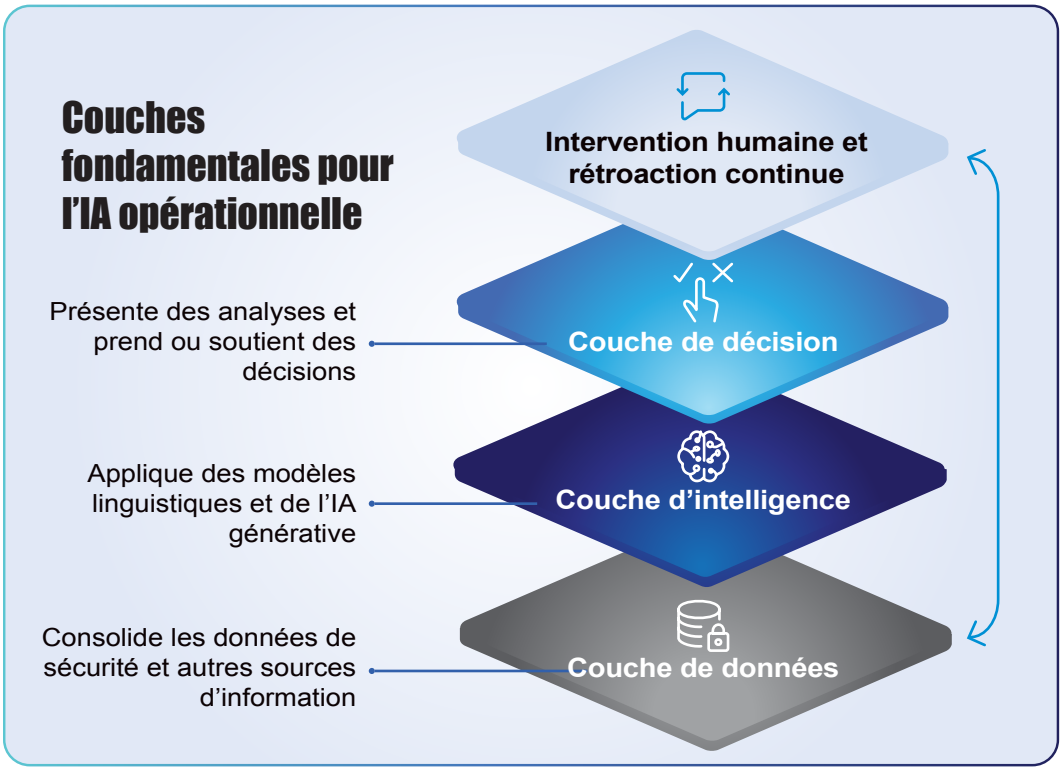
C. La couche décisionnelle

Analyser les données est une chose, prendre des décisions en fonction de celles-ci en est une autre. Au début de l'adoption de l'IA, la plupart des centres d'opérations ont préféré que l'IA présente des informations tout en laissant les décisions finales aux opérateurs humains. À mesure que la maturité augmente, les entreprises commencent à autoriser les systèmes d'IA à prendre certaines décisions prédéfinies ou présentant un faible risque de manière autonome. Au fil du temps, à mesure que les modèles d'IA et les structures de gouvernance évolueront, ces systèmes seront amenés à prendre des décisions plus complexes et reproductibles.

D. Rétroaction permanente et humain

Même dans les environnements basés sur l'IA, les humains restent essentiels. Leur rôle évolutif est centré sur la supervision, la compréhension contextuelle, la stratégie, les décisions à enjeux élevés et l'amélioration des systèmes d'IA.

La boucle de rétroaction est tout aussi essentielle. Au fur et à mesure que les incidents sont résolus et que leurs causes profondes sont identifiées, le fait de réintégrer ces informations dans le système garantit un apprentissage continu, ce qui accélère à chaque fois le rétablissement ou réduit le TMRS. Cela permet de minimiser les incidents récurrents et de renforcer la cohérence des réponses. Lorsque les équipes opérationnelles s'attaquent efficacement aux causes profondes, le volume d'incidents diminue, ce qui permet de consacrer du temps à des travaux d'IA proactifs et innovants qui améliorent la résilience et l'efficacité au sein du centre des opérations. Ensemble, ces composants clés permettent les opérations pilotées par l'IA nécessaires pour soutenir efficacement l'IA agentique.



Couches fondamentales à aborder

4. L'IA agentique dans les opérations de réseau et de sécurité

Le rôle de l'opérateur du centre d'exploitation du réseau (NOC) est très stressant, implique des délais serrés et consiste souvent à rechercher une aiguille dans une botte de foin. Le succès se mesure par le temps que prend une tâche. Avant l'introduction de l'IA agentique, les opérateurs du NOC devaient trouver des corrélations ou des problèmes similaires dans de vastes bases de données, afin de pouvoir localiser les problèmes récurrents et les données susceptibles de les aider à résoudre le problème en question. L'exemple ci-dessous illustre les avantages d'un partenariat avec une application d'IA agentique. L'agent peut aider à effectuer des recherches dans la base de données pour mieux identifier les problèmes passés, en tirer des enseignements, puis aider l'opérateur à résoudre le problème actuel non pas en quelques heures, mais en quelques minutes.

5. Impacts transformationnels sur les opérations de l'entreprise

Réfléchissez à ceci : il est 2 h 47 du matin lorsqu'un centre de commerce électronique mondial détecte des pics de latence dans les bases de données qui entravent le traitement des paiements. Le système de surveillance déclenche automatiquement l'alerte, mais l'IA agentique change tout.

De quelques heures à quelques minutes avec des agents IA

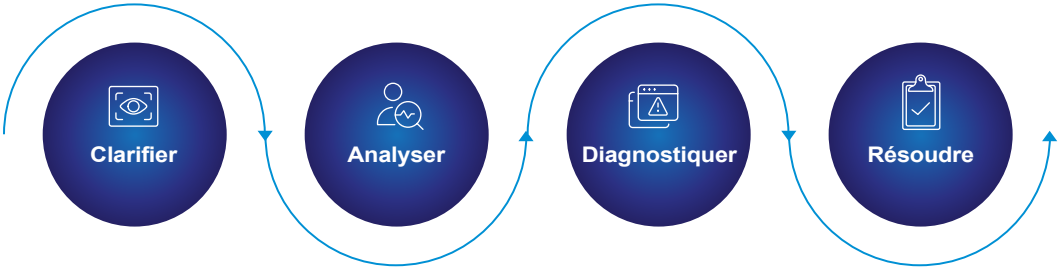
Clarifier : l'agent d'intelligence artificielle effectue immédiatement une corrélation automatique entre les événements du flot d'alertes, en distinguant la cause réelle (un conflit de tâches par lots) et tous les événements symptomatiques (pics de latence, erreurs de délai d'attente, sauvegardes de files d'attente). Au lieu de 20 alertes confuses, l'opérateur voit une image claire : « Conflit de base de données détecté ; cause première probable identifiée ».

Analyser : l'agent d'intelligence artificielle interroge les journaux de sécurité, la télémétrie réseau, les traces des applications et les bases de données de gestion des modifications, tout en recherchant simultanément des années de données historiques sur les incidents dans une base de données vectorielle. En quelques secondes, il détecte 847 modèles similaires et signale une correspondance de 89 % avec deux incidents antérieurs, en fonction de l'alignement des symptômes, du calendrier et des comportements du système. Cela montre une preuve irréfutable : le ticket de change CHG-45209 a modifié un calendrier de traitement par lots qui est désormais exécuté pendant les heures de pointe des transactions.

Diagnostiquer : l'IA ne se contente pas de trouver des corrélations ; elle en identifie la cause première en croisant le calendrier des traitements par lots avec les modèles de volume de transactions et indique exactement quand les choses se sont mal passées. Elle présente le diagnostic suivant : « Le traitement par lots 'user_analytics_aggregation_v2' entre en conflit avec le traitement des paiements en temps réel, selon le même schéma que les incidents #3421 et #11203. »

Résolution : C'est ici que l'humain intervient. L'agent AI propose trois options de résolution basées sur ce qui a réellement fonctionné auparavant, classées en fonction du taux de réussite et du risque. L'opérateur les passe en revue, prend en compte le contexte (il est 2 h 52, en dehors des fenêtres de maintenance) et prend la décision : suspendre le traitement par lots et configurer des annulations automatiques en cas de problème. L'IA exécute les actions approuvées tout en maintenant une surveillance continue.

Temps total entre l'alerte et la résolution : 14 minutes. Sans l'IA agentique, le même processus aurait pris plus de quatre heures.



L'IA agentique réduit le délai de résolution

L'IA agentique a pris en charge le gros du travail à chaque étape, notamment la corrélation automatisée, l'analyse intelligente, le diagnostic précis et la résolution guidée, mais l'humain a gardé le contrôle là où c'était le plus important : approuver le correctif. Cela a entraîné une réduction significative du TMRS. De plus, chaque incident traité de cette manière enrichit la base de données historique, ce qui rend les réponses futures encore plus précises.

Chaque centre d'opérations est mesuré à l'aide d'une série d'indicateurs de performance clés (KPI). Les indicateurs traditionnels se concentrent généralement sur la disponibilité des services, de nombreuses entreprises s'efforçant d'atteindre un temps de disponibilité de niveau Five Nines (99,999 %), ainsi que sur le volume d'incidents, y compris le nombre et la gravité des incidents majeurs et mineurs. Les autres mesures de base incluent le TMRS, l'objectif de temps de récupération (OTR) et l'objectif de point de restauration (OPR).

Bien que ces indicateurs soient importants, ils restent largement réactifs. Ils évaluent la capacité d'une équipe à réagir aux perturbations plutôt que l'efficacité avec laquelle elle les prévient. À mesure que l'IA s'intègre dans les opérations, les entreprises doivent commencer à intégrer des indicateurs proactifs. Par exemple :

- Combien d'incidents ont été détectés ou atténués par l'IA avant qu'ils ne dégénèrent ?
- À quelle vitesse les systèmes d'IA agentique ont-ils identifié les premiers indicateurs de défaillance ou de compromission ?
- Quel est le pourcentage du total des incidents gérés de manière autonome par les agents de l'IA ?

Mesurer séparément l'impact de l'IA agentique aide les entreprises à comprendre le véritable effet transformationnel de l'adoption. Le succès doit se traduire par des améliorations mesurables telles que :

- Une réduction du nombre total d'incidents, en particulier les plus graves
- Réduction des délais d'identification et de restauration à la suite d'incidents
- Résilience opérationnelle accrue grâce à une surveillance prédictive et à une réponse automatisée

L'IA générative et agentique permet de trouver l'aiguille dans la botte de foin, en découvrant rapidement les causes profondes et en permettant d'intervenir plus tôt.

L'évolution des opérations doit aller de pair avec l'adoption de l'IA. Trop souvent, les entreprises se concentrent sur le déploiement de modèles d'IA tout en négligeant de moderniser leurs centres d'opérations. Une équipe qui s'appuie sur la surveillance manuelle et les flux de traitement traditionnels ne peut pas suivre le rythme d'une entreprise qui évolue vers des opérations intelligentes basées sur l'IA.

En outre, alors que les acteurs de la menace utilisent de plus en plus l'IA pour automatiser et amplifier les cyberattaques, les centres d'opérations de sécurité doivent évoluer en parallèle, en tirant parti de l'IA pour maintenir la parité et se défendre à la vitesse des machines. Cette transformation n'est pas facultative ; elle est essentielle au maintien de la compétitivité, de la résilience et de la confiance à l'ère des opérations d'entreprise axées sur l'IA.

Dans cette nouvelle ère, la capacité à gérer efficacement les données organisationnelles est ce qui vous permettra en fin de compte de tirer le meilleur parti de l'IA. Il est essentiel de tirer parti de l'IA d'entreprise pour gérer, gouverner et optimiser en permanence les opérations de données. Alors que les centres d'opérations deviennent des centres névralgiques de l'innovation et de la résilience, la gestion des données et la stratégie doivent rester au cœur du programme de chaque direction. Les entreprises qui traitent les données non seulement comme une ressource, mais aussi comme un actif stratégique, et qui utilisent l'IA pour maintenir leur santé et leur disponibilité, seront les mieux placées pour exploiter tout le potentiel de transformation de l'IA à grande échelle.

Dans l'étude de cas suivante, un grand fabricant exploite le pouvoir des données pour mieux comprendre ses processus afin de réduire ses coûts et de réduire son recours au travail manuel.

Étude de cas

North Star BlueScope Steel

North Star BlueScope Steel

Filiale de la société australienne BlueScope, North Star BlueScope Steel produit et fournit des bandes en acier laminées à chaud pour les transformateurs de bobines, les producteurs de bandes laminées à froid, les fabricants de tuyaux et les tubes, les fabricants d'équipements d'origine et les centres de service en acier. Fondée en 1997, l'entreprise est le plus grand recycleur de ferraille de l'Ohio, recyclant près de 1,5 million de tonnes de ferraille chaque année.

North Star BlueScope Steel avait besoin d'un outil plus efficace pour mieux comprendre ses données de coûts et son flux de travail, afin de pouvoir l'utiliser pour interagir avec ses clients, effectuer des analyses de marché et établir des ventilations d'achats. La technologie devrait éliminer le processus manuel intensif et collecter automatiquement des données à partir de diverses sources, notamment les bases de données et les fours à arc électrique (FAE) de l'entreprise, ce qui lui permettrait de réaffecter le personnel et d'économiser des ressources, tout en répondant mieux aux besoins des clients.

L'entreprise a choisi d'utiliser des données et des analyses intelligentes pour accéder automatiquement aux données, les fusionner, les explorer et les analyser. La solution permet à North Star BlueScope Steel d'appliquer des algorithmes aux informations extraites afin de générer un rapport mensuel final, réduisant ainsi le recours au travail manuel. À l'aide de données et d'analyses, l'entreprise peut comparer les données mensuelles afin d'analyser comment des événements tels que les retards dans les usines et les blocages peuvent affecter la rentabilité. En adoptant l'IoT, l'entreprise espère intégrer des analyses dans les points de données provenant directement de ses instruments, afin d'analyser la consommation d'électricité, les conditions météorologiques, l'utilisation des matériaux et les prix de l'acier afin de mieux se faire une idée des besoins futurs et du potentiel de vente.

Télécharger The Fast Five

1. **Favorisez la transition vers des opérations autonomes.**
   Permettez à votre entreprise d'aller au-delà de la surveillance réactive en investissant dans des systèmes d'autoréparation basés sur l'IA qui préviennent les incidents de manière proactive et optimisent les performances.

2. **Favorisez la collaboration homme-IA.**
   Assurez-vous que vos équipes sont équipées pour travailler aux côtés de l'IA : établissez des cadres de gouvernance, renforcez la supervision humaine et créez des boucles de feedback continues pour optimiser à la fois la sécurité et l'innovation.

3. **Transformez les centres d'opérations en pôles d'innovation.**
   Transformez votre centre des opérations d'une fonction de support traditionnelle en un moteur stratégique pour l'innovation d'entreprise et le développement des talents, en en faisant un point central pour l'adoption et l'expérimentation de l'IA.

4. **Faites de l'adoption de l'IA une priorité au niveau du conseil d'administration.**
   Considérez l'intégration de l'IA dans les opérations comme un facteur de différenciation concurrentiel essentiel. Allouez l'attention et les ressources de la direction pour accélérer l'adoption, renforcer la sécurité et renforcer la confiance au cœur de l'entreprise.

5. **Redéfinissez les indicateurs de réussite pour l'ère de l'IA.**
   Dépassez les KPI réactifs traditionnels. Mettez en œuvre de nouvelles mesures qui suivent l'impact de l'IA - comme les incidents évités, la vitesse de réponse et les actions autonomes - pour mesurer précisément la valeur et favoriser l'amélioration continue.

Notes et références

[1] Foundry Research commandité par OpenText, "MarketPulse Survey: The Role of GenAI in Modernizing Content Management," mai 2025.

[2] Philip Miller, "Unlocking Unstructured Data: Fueling AI with Insights," *Dataversity,* 3 juin 2025, https://www.dataversity.net/articles/unlocking-unstructured-data-fueling-ai-with-insights/.

[3] Ibid.

[4] "More Than 80% of Enterprises Will Have Used Generative AI APIs or Deployed Generative AI Applications by 2026," *Gartner Press Release*, 11 Octobre 2023, www.gartner.com/en/newsroom/press-releases/2023-10-11-gartner-says-more-than-80-percent-of-enterprises-will-have-used-generative-ai-apis-or-deployed-generative-ai-enabled-applications-by-2026.

[5] "AI Governance Software Spend Will See 30% CAGR From 2024 to 2030," *Forrester Blog*, 13 novembre 2024, www.forrester.com/blogs/ai-governance-software-spend-will-see-30-cagr-from-2024-to-2030/.

[6] McKinsey & Company, "The State of AI in Early 2024: Gen AI Adoption Spikes and Starts to Generate Value," *QuantumBlack de McKinsey*, 30 mai 2024, www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-2024.

[7] Ibid.

[8] Accenture, "New Accenture Research Finds that Companies with AI-Led Processes Outperform Peers," *Accenture*, 10 octobre 2024, https://newsroom.accenture.com/news/2024/new-accenture-research-finds-that-companies-with-ai-led-processes-outperform-peers.

[9] "What is Artificial Intelligence (AI)?" *Organisation internationale de normalisation*, 31 janvier 2024, https://www.iso.org/artificial-intelligence/what-is-ai?.

[10] Melissa Russell, "How can I learn artificial intelligence?" *Harvard*, 8 avril 2025, https://extension.harvard.edu/blog/how-can-i-learn-artificial-intelligence/#What-is-Artificial-Intelligence.

[11] Sofia Samoili, Montserrat Lopez Cobo, Blagoj Delipetrev, Fernando Martinez-Plumed, Emilia Gomez Gutierrez, and Giuditta De Prato, "AI Watch, Defining Artificial Intelligence 2.0: Towards an operational definition and taxonomy for the AI Landscape," *Office des publications de l'Union européenne*, 2021.

[12] Ibid.

[13] Tim Mucci and Cole Stryker, "What is artificial superintelligence?" *IBM*, 22 juillet 2025, https://www.ibm.com/think/topics/artificial-superintelligence.

[14] Arend Hintze, "Understanding the four types of AI, from reactive robots to self-aware beings," *The Conversation*, 13 novembre 2016, https://theconversation.com/understanding-the-four-types-of-ai-from-reactive-robots-to-self-aware-beings-67616.

[15] A. M. Turing, "Computing Machinery and Intelligence," *Mind*, volume LIX, numéro 236, octobre 1950, https://doi.org/10.1093/mind/lix.236.433.

[16] J. McCarthy, M. L. Minsky, N. Rochester, & C.E. Shannon, "A proposal for the Dartmouth summer research project on artificial intelligence," *Dartmouth College*, 1955, https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/1904.

[17] Ben Lutkevich, "What is AI Winter? Definition, History and Timeline," *Tech Target*, 26 août 2024, https://www.techtarget.com/searchenterpriseai/definition/AI-winter.

[18] D. Crevier, *AI : L'histoire tumultueuse de la recherche de l'intelligence artificielle*, Basic Books, 1993.

[19] Ibid.

[20] S.J. Russell et P. Norvig, *Intelligence artificielle : une approche moderne*, 4e éd. , Pearson, 2021.

[21] Yann LeCun, Yoshua Bengio, and Geoffrey Hinton, "Deep learning," *Nature*, 521 (7553), 436—444, 2015, https://doi.org/10.1038/nature14539.

[22] Melissa Russell, "How can I learn artificial intelligence?" *Harvard*, 8 avril 2025, https://extension.harvard.edu/blog/how-can-i-learn-artificial-intelligence/#What-is-Artificial-Intelligence.

[23] "Gartner Survey Reveals GenAI Attacks Are on the Rise," *Gartner Inc.*, 2025-09-22, https://www.gartner.com/en/newsroom/press-releases/2025-09-22-gartner-survey-reveals-generative-artificial-intelligence-attacks-are-on-the-rise.

[24] Akshay Joshi, Giulia Moschetta, and Ellie Winslow, "Global Cybersecurity Outlook 2025 Insight Report," *Forum économique mondial en collaboration avec Accenture*, janvier 2025, https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.

[25] Shuli Jiang, Swanand Ravindra Kadhe, Yi Zhou, Ling Cai, and Nathalie Baracaldo, "Forcing Generative Models to Degenerate Ones: The Power of Data Poisoning Attacks," *Université Cornell*, arXiv:2312.04748, 7 décembre 2023, https://arxiv.org/abs/2312.04748.

[26] BB. Biggio, B. Nelson, and P. Laskov, "Poisoning Attacks Against Support Vector Machines," *Proceedings of the 29th International Conference on Machine Learning (ICML)*, 2012.

[27] Tianyu Gu, Brendan Dolan-Gavitt, and Siddharth Garg, "BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain," *Cornel University*, arXiv:1708.06733, 11 mars 2019, https://arxiv.org/abs/1708.06733.

[28] Ian J. Goodfellow, Jonathon Shlens, and Christian Szegedy, "Explaining and Harnessing Adversarial Examples," *Université Cornell*, arXiv:1412.6572, 20 mars 2015, https://arxiv.org/abs/1412.6572.

[29] Wencheng Yang, Song Wang, Di Wu et al, "Deep Learning Model Inversion Attacks and Defenses: A Comprehensive Survey," *Université Cornell,* arXiv:2501.18934, 30 avril 2025, https://arxiv.org/abs/2501.18934.

[30] Ninareh Mehrabi, Fred Morstatter, Nripsuta Saxena, Kristina Lerman, and Aram Galstyan, "A Survey on Bias and Fairness in Machine Learning, *Université Cornell*, arXiv:1908.09635, 25 janvier 2022, https://arxiv.org/abs/1908.09635.

[31] ISO/IEC 27001:2022, "Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements," International Organization for Standardization.

[32] Sandeep Kumar Jangam, "Importance of Encrypting Data in Transit and at Rest Using TLS and Other Security Protocols and API Security Best Practices," *International Journal of AI, BigData, Computational and Management Studies*, 4 (3), 82—91, 2023, https://ijaibdcms.org/index.php/ijaibdcms/article/view/242/.

[33] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong, "Federated Machine Learning: Concept and Applications," *bibliothèque numérique ACM*, 28 janvier 2019, https://dl.acm.org/doi/10.1145/3298981.

[34] Parlement et Conseil européen, Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel – Article 17 (Droit à l'effacement), 2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[35] Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly, "Zero Trust Architecture," *publication spéciale du NIST 800-207*, août 2020, https://doi.org/10.6028/NIST.SP.800-207.

[36] Alexey Kurakin, Ian Goodfellow, and Samy Bengio, "Adversarial Machine Learning at Scale," *Université Cornell*, arXiv:1611.01236, 11 février 2017, https://arxiv.org/abs/1611.01236.

[37] Yusuke Uchida, Yuki Nagai, Shigeyuki Sakazawa, and Shin'ichi Satoh, "Embedding Watermarks into Deep Neural Networks," *Université Cornell*, arXiv:1701.04082, 20 avril 2017, https://arxiv.org/abs/1701.04082.

[38] Forrester. "AI Governance Software Spend Will See 30 % CAGR From 2024 to 2030." *Forrester Research*, 13 novembre 2024, https://www.forrester.com/blogs/ai-governance-software-spend-will-see-30-cagr-from-2024-to-2030/.

[39] "Information Governance Reference Model," EDRM, http://www.edrm.net/projects/igrm.

[40] "Key Regulatory and Industry Initiatives," *Capgemini*, https://web.archive.org/web/20141105171058/https://www.worldpaymentsreport.com/kriis#Heat-Map-of-KRIIs-Global-and-Regional.

[41] Gartner, Inc., "Gartner Poll Finds 55% of Organizations Have an AI Board," *Press Release*, 26 juin 2024, https://www.gartner.com/en/newsroom/press-releases/2024-06-26-gartner-poll-finds-55-percent-of-organizations-have-an-ai-board.

[42] Ibid.

[43] Alex Edquist, Liz Grennan, Sian Griffiths, and Kayvaun Rowshankish, "Data ethics: What it means and what it takes," *McKinsey & Company*, 23 septembre 2022, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/data-ethics-what-it-means-and-what-it-takes.

[44] James Moor, "What is Computer Ethics?" *Métaphilosophie*, 16 (4), 266—275, 1985, https://doi.org/10.1111/j.1467-9973.1985.tb00173.x.

[45] Unesco, "Recommendation on the Ethics of Artificial Intelligence," *UNESCO.org*, 2022, https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence.

[46] Ibid.

[47] Ibid.

[48] OECD, "Recommendation of the Council on Artificial Intelligence," OECD/LEGAL/0449, 2019.

[49] Commission européenne, "Regulation (EU) 2024/1689 on Artificial Intelligence," 2024.

[50] NIST, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," *NIST Special Publication AI 100-1*, 2023.

[51] Dario Maisto, "From Digital Sovereignty Platforms To Sovereign Cloud Platforms: Three Reasons For A Title Change," *Forrester Blogs*, 11 août 2025, www.forrester.com/blogs/from-digital-sovereignty-platforms-to-sovereign-cloud-platforms-three-reasons-for-a-title-change.

[52] McKinsey & Company, "Future-Proofing the IT Function Amid Global Trends and Disruptions," *McKinsey Digital*, 11 juin 2024, www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/future-proofing-the-it-function-amid-global-trends-and-disruptions.

[53] Sébastien Bubeck, Varun Chandrasekaran, Ronen Eldan et al, "Sparks of artificial general intelligence: Early experiments with GPT-4," *Université Cornell*, 13 avril 2023, https://arxiv.org/abs/2303.12712.

[54] Aditya Challapally, Chris Pease, Ramesh Raskar, et al., "The GenAI Divide: State of AI in Business 2025," *MIT NANDA*, juillet 2025, https://mlq.ai/media/quarterly_decks/v0.1_State_of_AI_in_Business_2025_Report.pdf.

[55] Mark J. Barrenechea, Tom Jenkins, and David Fraser, *The Anticipant Organization*, OpenText Corporation, 2022.

[56] Ibid.

[57] Ibomoiye Domor Mienye, Nobert Jere, George Obaido, Oyindamola Omolara Ogunruku, Ebenezer Esenogho and Cameron Modisane, "Large language models: an overview of foundational architectures, recent trends, and a new taxonomy," *Discover Applied Sciences*, 7, 1027, 2 septembre 2025, https://link.springer.com/article/10.1007/s42452-025-07668-w.

[58] Ruei-Shan Lu ,Ching-Chang Lin , and Hsiu-Yuan Tsao, "Empowering Large Language Models to Leverage Domain-Specific Knowledge in E-Learning," *Applied Sciences, 14 (12), 5264*, 18 juin 2024, https://doi.org/10.3390/app14125264.

[59] Qizheng Zhang, Changran Hu, Shubhangi Upasani et al. "Agentic Context Engineering: Evolving Contexts for Self-Improving Language Models," prépublication d'arXiv arXiv:2510.04618, 2025, https://www.arxiv.org/pdf/2510.04618.

[60] Lingrui Mei, Jiayu Yao, Yuyao Ge et al, "A survey of context engineering for large language models," Université Cornell, arXiv:2507.13334, 21 juillet 2025, https://arxiv.org/abs/2507.13334.

[61] A. Feder Cooper, Christopher A. Choquette-Choo, Miranda Bogen et al. "Machine Unlearning Doesn't Do What You Think: Lessons for Generative AI Policy, Research, and Practice," SSRN, 6 février 2025, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5060253.

[62] K. Boyd, "Microsoft 365 copilot for executives: Sharing Our Customer Zero Deployment and adoption journey at Microsoft," *blog Microsoft Inside Track*, 5 décembre 2024, https://www.microsoft.com/insidetrack/blog/copilot-for-microsoft-365-for-executives-sharing-our-internal-deployment-and-adoption-journey-at-microsoft/.

[63] Propriétaire du produit. Scaled Agile Framework, 25 février 2025, https://framework.scaledagile.com/product-owner.

[64] Alexander Sukharevsky, Alexis Krivkovich, Arne Gast, et al, "The agentic organization: Contours of the next paradigm for the AI era," *McKinsey & Company*, September 26, 2025, https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-agentic-organization-contours-of-the-next-paradigm-for-the-ai-era.

[65] V.L. Sunkara, "KPIs for AI agents and Generative AI: A rigorous framework for evaluation and Accountability," *Revue internationale de recherche scientifique et de technologie moderne*, 22-29, 2024, https://doi.org/10.38124/ijsrmt.v3i4.572.

[66] Jared Kaplan, Sam McCandlish, Tom Henighan et al, "Scaling Laws for Neural Language Models," *Université Cornell*, arXiv:2001.08361, 23 janvier 2020, https://arxiv.org/abs/2001.08361.

[67] Gary Marcus, "Deep learning is hitting a wall", *Communications of the ACM*, 65 (8), 36-43, 2022, https://nautil.us/deep-learning-is-hitting-a-wall-238440/.

[68] Annette Zimmermann and Danielle Casey, "Emerging Tech Impact Radar: Generative AI," *Gartner*, 14 février 2025.

Glossaire

Accès auditable : capacité d'un système à enregistrer et à vérifier qui a accédé aux ressources, quand et comment. Cela garantit la responsabilité et la conformité en permettant de vérifier et de retracer les activités d'accès si nécessaire.

Accès extraterritorial : capacité des gouvernements, des organisations ou des entités à accéder et à demander l'accès aux données stockées en dehors de leur propre juridiction nationale. En matière de technologie et de gouvernance des données, l'accès extraterritorial soulève des inquiétudes quant à la souveraineté, à la confidentialité et à la conformité, car il permet à des lois telles que le CLOUD Act des États-Unis ou des cadres similaires d'obliger la divulgation de données stockées à l'étranger.

Air Gap ou Isolation par air : Mesure de sécurité du réseau mise en œuvre sur un ou plusieurs ordinateurs. Il vise à garantir qu'un réseau informatique sécurisé est physiquement déconnecté de tous les réseaux non sécurisés à sa portée. Les réseaux non sécurisés peuvent inclure Internet ou d'autres réseaux locaux. Cette méthode est souvent utilisée dans des environnements à haute sécurité, tels que ceux de l'armée. Ce terme est aussi parfois appelé « isolation par air » ou « système isolé ».

Agent IA : un système logiciel spécifique conçu pour une tâche définie qui peut percevoir de manière autonome son environnement, planifier et réfléchir sur les tâches, et prendre des mesures pour atteindre des objectifs précis. Il fonctionne avec un certain degré d'indépendance (mais généralement dans le cadre de contraintes définies par l'homme), apprend ou s'adapte au fil du temps, utilise des outils ou des sources de données externes en cas de besoin et soutient la prise de décision avec un minimum de supervision directe. Les agents d'IA sont les « éléments de base » du cadre de « l'IA agentique ».

Analyse d'impact relative à la protection des données (AIDP) : processus requis par des réglementations telles que le RGPD pour identifier et minimiser les risques liés aux données personnelles avant de démarrer un projet impliquant leur collecte ou leur traitement. Une AIPD évalue la manière dont les données seront utilisées, évalue les impacts potentiels sur la confidentialité et documente les mesures de protection pour garantir la conformité et protéger les droits des individus.

Analytique : processus systématique de collecte, de traitement et d'interprétation des données afin d'identifier des modèles, des tendances et des enseignements. En informatique, les analyses de données sont utilisées pour soutenir la prise de décision, optimiser les performances et prévoir les résultats futurs grâce à des techniques telles que l'analyse statistique, la visualisation des données et l'apprentissage automatique.

Analytique en temps réel : processus de collecte, de traitement et d'analyse des données dès leur génération, permettant aux organisations d'obtenir des informations et de prendre des décisions sans délai. Dans le domaine de l'informatique, l'analytique en temps réel prend en charge des cas d'utilisation tels que la détection des fraudes, les recommandations personnalisées, la surveillance du système et le suivi des performances en temps réel. (Voir également : Analyses).

Analytique pilotée par l'IA : application de l'intelligence artificielle et de l'apprentissage automatique pour automatiser la collecte, la préparation et l'analyse des données. En découvrant des modèles et en générant des informations en temps réel ou quasi réel, il aide les organisations à prévoir les résultats, à identifier les tendances et à prendre des décisions plus rapides et plus éclairées.

Apprentissage automatique (AA) : domaine de l'intelligence artificielle qui se concentre sur le développement d'algorithmes et de modèles permettant aux systèmes d'apprendre à partir des données et d'améliorer leurs performances au fil du temps sans être explicitement programmés. L'apprentissage automatique est utilisé pour identifier des modèles, faire des prédictions et soutenir la prise de décision dans des applications telles que les moteurs de recommandation, la détection des fraudes, la reconnaissance d'images et le traitement du langage naturel.

Apprentissage profond : branche spécialisée de l'apprentissage automatique qui repose sur des réseaux neuronaux profonds, c'est-à-dire des structures multicouches de « neurones » interconnectés dont les poids et les paramètres peuvent être ajustés grâce à l'entraînement. Cette approche excelle dans l'extraction de modèles et d'informations à partir de données non structurées telles que les images, le texte, l'audio et la vidéo, ce qui en fait l'épine dorsale de nombreuses applications d'IA modernes telles que la reconnaissance d'images, la traduction linguistique et le traitement de la parole.

Architecture monolithique : conception logicielle traditionnelle dans laquelle tous les composants d'une application, tels que l'interface utilisateur, la logique métier et la gestion des données, sont étroitement intégrés et déployés en une seule unité. Bien que plus simples à créer au départ, les systèmes monolithiques peuvent être plus difficiles à dimensionner, à mettre à jour ou à adapter que les alternatives composables.

Audit : examen et évaluation systématiques des systèmes, des processus ou des données informatiques pour garantir l'exactitude, la sécurité, la conformité et le bon fonctionnement. Elles peuvent consulter les journaux, les contrôles d'accès, les configurations et les politiques afin de détecter les irrégularités, de confirmer le respect des normes et d'identifier les domaines à améliorer.

Autorisations : gestion des personnes autorisées à accéder à un ordinateur ou à un réseau. La liste de contrôle d'accès (LCA) est l'ensemble des données associées à un fichier, un répertoire ou une autre ressource qui définit les autorisations dont disposent les utilisateurs, les groupes, les processus ou les périphériques pour y accéder.

Automatisation : utilisation de la technologie pour effectuer des tâches avec une intervention humaine minimale ou nulle. Dans le domaine de l'informatique, l'automatisation rationalise les processus répétitifs ou basés sur des règles, tels que le déploiement de logiciels, la surveillance du système ou le traitement des données, afin d'améliorer l'efficacité, la cohérence et la fiabilité.

Automatisation des flux de traitement : sous-ensemble de l'automatisation qui se concentre sur la coordination et l'exécution d'une série de tâches ou de processus entre les systèmes, les applications ou les équipes. L'automatisation des flux de traitement décrit les étapes d'un processus métier ou technique et utilise l'automatisation pour garantir qu'elles sont exécutées dans le bon ordre avec un minimum de saisie manuelle.

Automatisation robotique des processus (ARP) : technologie logicielle qui automatise les tâches commerciales structurées et basées sur des règles en imitant les actions humaines dans les systèmes numériques. L'ARP interagit avec les applications, les formulaires et les données comme le ferait un utilisateur (en cliquant, en tapant, en copiant et en déplaçant des informations), mais avec rapidité, cohérence et précision. Elle est couramment utilisée pour rationaliser les processus administratifs volumineux tels que la saisie de données, le traitement des factures et la gestion des enregistrements. Dans l'entreprise, l'ARP devient encore plus puissante lorsqu'elle est associée à l'IA et à l'orchestration des flux de traitement, permettant à la fois l'automatisation des tâches et une aide à la décision intelligente à grande échelle.

Axé sur les données : utilisation de l'analyse des données et des informations pour éclairer les décisions et les stratégies commerciales.

Big Data : ensembles de données extrêmement volumineux et complexes qui nécessitent des outils et des analyses avancés pour être traités et en extraire des enseignements.

Bots/Robots : logiciels conçus pour automatiser les tâches, souvent en simulant l'activité humaine. En informatique, les robots peuvent exécuter un large éventail de fonctions, allant d'activités utiles telles que les robots conversationnels de support client, l'indexation des moteurs de recherche et l'automatisation des flux de traitement, à des utilisations malveillantes telles que courriels indésirables, attaques par bourrage d'identifiants ou diffusion de logiciels malveillants. Les bots fonctionnent généralement à grande vitesse et à grande échelle, ce qui en fait des outils puissants, tant pour des usages légitimes que nuisibles.

California Consumer Privacy Act (CCPA) : Loi sur la confidentialité des données promulguée en Californie en 2020 qui donne aux résidents un meilleur contrôle sur leurs informations personnelles. La CCPA oblige les entreprises à divulguer les données qu'elles collectent, comment elles sont utilisées et avec qui elles sont partagées, tout en accordant aux consommateurs le droit d'accéder à leurs données, de les supprimer et de s'opposer à leur vente.

Cartographie des données : processus qui consiste à faire correspondre les champs de données d'un système, d'un format ou d'une base de données à un autre afin de permettre l'intégration, la migration ou l'analyse. Une cartographie efficace des données garantit la cohérence et la précision, ce qui permet de consolider les informations entre les plateformes, de garantir la conformité et de préparer les données pour l'e ou l'apprentissage automatique.

Chiffrement : processus de conversion des données dans un format codé à l'aide d'algorithmes et de clés cryptographiques pour empêcher tout accès non autorisé. En informatique, le chiffrement garantit que seules les parties autorisées disposant de la bonne clé peuvent déchiffrer et lire les informations, protégeant ainsi les données sensibles pendant le stockage ou la transmission.

Cloud privé : environnement cloud dédié à une seule organisation, offrant un accès exclusif à l'infrastructure, aux ressources et aux services. Les clouds privés peuvent être hébergés sur site ou par un fournisseur tiers et sont conçus pour offrir un contrôle, une sécurité et une personnalisation accrus par rapport aux environnements de cloud public. (Voir également : cloud public).

Cloud public : modèle de cloud dans lequel l'infrastructure, les ressources et les services sont détenus et exploités par un fournisseur tiers et fournis via Internet. Les environnements de cloud public sont partagés entre plusieurs organisations (locataires), mais les données et les charges de travail restent logiquement séparées. Ils offrent évolutivité, flexibilité et rentabilité. Des exemples courants sont Amazon Web Services (AWS), Microsoft Azure et Google Cloud. (Voir également : Cloud privé).

Cloud/Le cloud : modèle informatique qui fournit un accès à la demande à des ressources partagées, telles que les serveurs, le stockage, les bases de données, les réseaux, les logiciels et les outils d'analyse, via Internet. Le cloud permet aux utilisateurs et aux entreprises de faire évoluer rapidement les ressources, de ne payer que pour ce qu'ils utilisent et d'accéder aux services sans avoir à gérer de matériel physique ou d'infrastructure sur site.

CloudOps ou Opérations Cloud : abréviation de Cloud Operations, CloudOps se concentre sur la gestion et l'optimisation des applications et des infrastructures exécutées dans des environnements informatiques cloud. Il étend les principes de DevOps au cloud, en mettant l'accent sur la scalabilité, la surveillance des performances, la sécurité et l'efficacité des coûts dans des systèmes dynamiques et distribués.

Commerce électronique : l'achat et la vente de biens ou de services sur Internet, y compris des activités telles que les achats en ligne, les paiements électroniques, les marchés numériques et le commerce mobile. Le commerce électronique permet aux entreprises d'atteindre leurs clients directement par le biais de sites Web, d'applications et de plateformes, transformant ainsi la façon dont les produits sont commercialisés, achetés et livrés.

Confidentialité : protection et traitement approprié des données des utilisateurs afin de garantir que les individus gardent le contrôle sur la manière dont leurs informations personnelles sont collectées, utilisées, partagées et stockées dans les environnements informatiques. Les mesures de protection de la vie privée empêchent l'accès non autorisé ou l'utilisation abusive des données et sont régies par des normes légales, éthiques et réglementaires. (Voir également : Informations personnelles identifiables/IPI).

Confidentialité dès la conception : cadre qui intègre les principes de confidentialité et de protection des données directement dans la conception et le fonctionnement des technologies, des processus et des systèmes. Il met l'accent sur les mesures proactives, telles que la minimisation de l'utilisation des données, la sauvegarde par défaut et la garantie de la transparence, afin que la confidentialité ne soit pas une question secondaire, mais un élément essentiel de conception.

Confidentialité des données : discipline qui consiste à gérer et à protéger les informations personnelles afin de garantir qu'elles sont collectées, stockées et utilisées de manière à respecter les droits et les attentes des individus. La confidentialité des données met l'accent sur la transparence, le consentement et la conformité légale, afin de garantir que les entreprises gèrent les données sensibles de manière responsable tout en préservant la confiance des utilisateurs. (Voir également : Sécurité des données ; Cybersécurité ; Conformité).

Conformité (en technologie) : pratique qui consiste à s'assurer que les systèmes, les processus et la gestion des données sont conformes aux lois, réglementations, normes et politiques internes établies. Dans le domaine de la technologie, la conformité couvre souvent des domaines tels que la confidentialité des données (par exemple, le RGPD, le CCPA), la cybersécurité, l'accessibilité et les règles spécifiques au secteur, aidant les organisations à réduire les risques, à maintenir la confiance et à éviter les sanctions légales ou financières. (Voir également : sécurité des données ; cybersécurité ; confidentialité des données).

Couche d'intelligence : niveau analytique et décisionnel au sein d'une pile technologique qui transforme les données brutes en informations exploitables. Souvent alimentée par l'IA, l'apprentissage automatique ou des analyses avancées, la couche d'intelligence se situe au-dessus des systèmes de stockage et de traitement des données, permettant la personnalisation, les prévisions et l'automatisation qui permettent d'obtenir des résultats commerciaux plus intelligents.

Couche d'orchestration : couche de gestion informatique qui automatise la coordination, la planification et l'exécution de tâches complexes sur plusieurs systèmes, applications ou services. La couche d'orchestration garantit que les composants fonctionnent parfaitement ensemble en gérant les flux de traitement, l'allocation des ressources, le dimensionnement et les dépendances. Elle est couramment utilisée dans les environnements cloud, les applications conteneurisées et les microservices pour rationaliser les activités et réduire les interventions manuelles.

Couche logicielle intermédiaire (couche intergicielle) : logiciel qui agit comme un pont entre les systèmes d'exploitation, les bases de données et les applications, leur permettant de communiquer et de partager des données efficacement. La couche intergicielle fournit des services communs tels que la messagerie, l'authentification, la gestion des API et le traitement des transactions, simplifiant ainsi l'intégration et l'interopérabilité entre les systèmes complexes.

Cybersécurité : pratique qui consiste à protéger les systèmes, les réseaux, les logiciels et les données contre les attaques numériques, les accès non autorisés ou les dommages. Cela englobe des technologies, des processus et des politiques qui protègent la confidentialité, l'intégrité et la disponibilité, aidant ainsi les organisations à se défendre contre les menaces telles que les logiciels malveillants l'hameçonnage (phishing), les rançongiciels (ransomwares) et les risques internes. (Voir également : sécurité des données ; conformité ; confidentialité des données).

Données non structurées : données qui ne résident pas dans des emplacements fixes. Le texte en format libre dans un document de traitement de texte est un exemple typique.

Données structurées : données qui se trouvent dans des champs fixes au sein d'un enregistrement ou d'un fichier. Les bases de données relationnelles et les feuilles de calcul sont des exemples de données structurées.

Données Zero-Party : informations partagées volontairement par les utilisateurs, telles que les préférences ou les intentions, collectées par le biais d'enquêtes ou de questionnaires.

DevOps : ensemble de pratiques qui combinent le développement logiciel (Dev) et les opérations informatiques (Ops) pour raccourcir les cycles de développement, améliorer la collaboration et fournir des mises à jour de manière plus fiable. En automatisant les tests, l'intégration et le déploiement, DevOps aide les équipes à publier des logiciels plus rapidement tout en préservant la qualité.

Droits et autorisations : identifie les circonstances dans lesquelles un actif particulier peut être utilisé. Par exemple, il indique qui est légalement propriétaire de l'actif, sur quels supports il peut être utilisé (Web, imprimé, T5) et les passifs financiers encourus pour inclure l'actif.

Échange de données informatisé (EDI) : méthode normalisée d'échange électronique de documents commerciaux, tels que les bons de commande, les factures et les avis d'expédition, entre les organisations, éliminant la saisie manuelle des données et améliorant la rapidité, la précision et la cohérence des transactions.

Entrepôt de données : système de stockage structuré optimisé pour les requêtes et les rapports sur des données sélectionnées. Contrairement aux lacs de données, qui contiennent des données brutes, les entrepôts de données stockent des données nettoyées, organisées et intégrées, généralement provenant de sources multiples, ce qui permet aux entreprises d'exécuter plus facilement des analyses, de générer des tableaux de bord et de soutenir la prise de décision.

Évolutivité : capacité d'un système, d'une application ou d'une infrastructure à gérer l'augmentation des charges de travail ou des demandes en ajoutant des ressources telles que la puissance de traitement, la mémoire ou le stockage. En informatique, l'évolutivité garantit des performances et une fiabilité constantes à mesure que l'utilisation augmente et peut s'appliquer à la montée en puissance (scalabilité verticale) ou à l'extension (scalabilité horizontale).

FinOps : abréviation de Cloud Financial Operations (Opérations financières dans le cloud), FinOps est un cadre permettant de gérer les coûts liés au cloud grâce à la collaboration entre les équipes d'ingénierie, de finance et commerciales. Il garantit la responsabilité financière, optimise les dépenses et aide à prendre des décisions éclairées en équilibrant performance et coûts dans les environnements cloud.

Géopolitique : étude de la façon dont les facteurs géographiques, tels que l'emplacement, les ressources, le terrain physique, la population et les tendances économiques ou démographiques, influencent le pouvoir politique, la politique étrangère et la prise de décision entre les états ou d'autres acteurs politiques. La géopolitique examine comment le contrôle du territoire, des régions stratégiques et des caractéristiques géographiques façonne les relations, les conflits et la coopération sur la scène mondiale.

Gestion de contenu d'entreprise (GCE) : la GCE est une plateforme qui stocke, gère et diffuse du contenu au niveau de l'entreprise. Cela inclut les documents, les images, les vidéos et les autres formes de contenu qui sont importants pour une organisation. Une plateforme GCE doit s'intégrer parfaitement aux applications et systèmes essentiels de l'entreprise (tels que la planification des ressources d'entreprise, la gestion de la relation client, la gestion du capital humain et les solutions de gestion de la chaîne d'approvisionnement) afin d'accélérer les processus commerciaux et de tirer parti des données qu'ils génèrent. La GCE inclut une gestion de contenu cloud qui peut être rapidement déployée pour permettre aux entreprises de stocker, de gérer et de collaborer avec du contenu numérique dans le cloud.

Gestion de la configuration : processus qui consiste à gérer systématiquement les modifications apportées à un système afin de maintenir son intégrité, sa cohérence et sa traçabilité tout au long de son cycle de vie.

Gestion de la relation client (CRM) : stratégie et ensemble d'outils logiciels qui aident les entreprises à gérer les interactions avec leurs clients actuels et potentiels. Les systèmes CRM centralisent les données clients, suivent les ventes et les communications, et soutiennent le marketing, le service et l'établissement de relations afin d'améliorer la fidélisation et de stimuler la croissance.

Gestion des identités : composante essentielle de la gestion des identités et des accès (GIA) axée sur la création, la maintenance et la suppression des identités des utilisateurs et de leurs attributs. Alors que la GIA supervise à la fois les contrôles d'identité et d'accès, la gestion des identités gère spécifiquement les tâches liées au cycle de vie de l'identité des utilisateurs, telles que le provisionnement des comptes, la mise à jour des rôles des utilisateurs et la garantie de l'exactitude et de la sécurité des données d'identité.

Gestion des identités et des accès (Identity and Access Management/IAM) : cadre de sécurité qui garantit que les bonnes personnes disposent de l'accès approprié aux bonnes ressources au bon moment. Il gère les identités numériques, l'authentification et les autorisations sur l'ensemble des systèmes et des applications afin de protéger les données sensibles et de garantir la conformité.

Gestion des informations d'entreprise (EIM) : les solutions de gestion des informations d'entreprise gèrent la création, la capture, l'utilisation et le cycle de vie éventuel des informations structurées et non structurées. Elles sont conçues pour aider les entreprises à valoriser leurs informations, à les sécuriser et à répondre à la liste croissante des exigences de conformité.

Gestion des processus : automatisation des processus métier à l'aide d'un système expert basé sur des règles qui utilise les outils appropriés et fournit les informations, les listes de contrôle, les exemples et les rapports d'état nécessaires à l'utilisateur.

Gestion des processus d'entreprise (GPE) : fait référence à l'alignement des processus sur les objectifs stratégiques d'une organisation, à la conception et à la mise en œuvre d'outils ou d'architectures centrés sur les processus, et à la détermination de systèmes de mesure pour une gestion efficace des processus.

Gestion du changement : discipline à champ large qui met l'accent sur l'aspect humain et organisationnel du changement, garantissant que les nouveaux systèmes, processus ou technologies sont adoptés avec succès. Alors que la gestion de la configuration traite de la cohérence technique, la gestion du changement concerne la communication, la formation et l'alignement des parties prenantes afin de minimiser les résistances et de maximiser la valeur des initiatives de changement.

Gestion du cycle de vie du contenu (Content Lifecycle Management/CLM) : combinaison de la gestion des documents, de la gestion des enregistrements, du flux de traitement, de l'archivage et de l'imagerie dans une solution entièrement intégrée pour gérer efficacement le cycle de vie du contenu, de sa création à son archivage et à sa suppression éventuelle.

Gouvernance numérique : cadre des politiques, des rôles, des processus et des normes qui guident la manière dont une organisation gère ses actifs, ses technologies et ses données numériques. Il garantit la responsabilité, la conformité, la sécurité et l'alignement sur les objectifs commerciaux tout en équilibrant l'innovation et la gestion des risques dans les opérations numériques.

Humain dans la boucle (Human-in-the-Loop/HITL) : approche de l'intelligence artificielle et de l'automatisation dans laquelle les humains restent activement impliqués dans le processus de prise de décision ou de formation du système. HITL est utilisé pour assurer la supervision, améliorer la précision, corriger les erreurs et traiter les cas critiques, en veillant à ce que les systèmes automatisés soient conformes au jugement humain, à l'éthique et au contexte du monde réel.

Hyperscaler : un grand prestataire de services cloud – comme Amazon Web Services (AWS), Microsoft Azure ou Google Cloud – qui fournit des services de calcul, de stockage et de mise en réseau à grande échelle dans des centres de données mondiaux. Les hyperscalers sont connus pour leur capacité à augmenter ou à diminuer instantanément les ressources, à prendre en charge les charges de travail mutualisées et à fournir l'infrastructure essentielle des applications natives du cloud, de l'IA et des traitements intensifs de données.

IA d'entreprise (IAE) : application rigoureuse de l'intelligence artificielle au sein d'une organisation pour résoudre des problèmes métiers concrets, améliorer la prise de décision et automatiser les tâches de manière sécurisée et à grande échelle. Il ne s'agit pas d'une catégorie distincte d'intelligence, mais du déploiement gouverné des capacités d'IA existantes - notamment l'apprentissage automatique, le traitement du langage naturel, la vision par ordinateur, l'automatisation et l'IA générative - dans un environnement de données structurées et de conformité. L'IA d'entreprise dépend d'informations fiables, de contrôles souverains des données, de la gestion du cycle de vie (MLOps et LLMOps), d'une infrastructure cloud hybride ou souveraine et de couches d'orchestration sécurisées pour garantir que l'IA fonctionne de manière responsable, transparente et fiable dans l'ensemble de l'entreprise.

IA de raisonnement : systèmes d'IA qui appliquent la pensée logique, la planification étape par étape, la résolution de problèmes et la prise de décision à l'aide de données structurées ou non structurées, allant au-delà de la reconnaissance des formes pour tirer des conclusions et résoudre des problèmes complexes.

IA générative (GenAI) : des systèmes d'IA qui créent de nouveaux contenus originaux en utilisant des modèles d'apprentissage automatique. Des modèles tels que ChatGPT, Claude, Gemini et DeepSeek sont formés sur des sources de données publiques telles que les sites Web, les actualités, Reddit et Wikipedia. Bien que les modèles GenAI soient utiles pour générer des informations générales, ils sont limités aux tâches générales. Cela s'explique par le fait qu'ils n'ont pas accès aux données privées en temps réel de l'entreprise, requises pour des cas d'utilisation professionnels spécifiques.

Indicateurs de performance clé (IPC) : mesures quantifiables utilisées pour évaluer l'efficacité avec laquelle une organisation, une équipe ou un processus atteint ses objectifs. Les IPC suivent les progrès réalisés par rapport aux objectifs stratégiques, orientent la prise de décision et peuvent aller de mesures financières telles que la croissance du chiffre d'affaires à des mesures opérationnelles telles que la fidélisation des clients ou la disponibilité du système.

Informations personnelles identifiables (IPI) : toutes données qui peuvent être utilisées pour identifier un individu, seules ou combinées à d'autres informations. Les exemples incluent les noms, les adresses, les numéros de téléphone, les adresses courriel, les numéros de sécurité sociale ou de passeport, ainsi que les dossiers financiers ou médicaux. Dans le domaine de l'informatique et de la confidentialité des données, la protection des informations personnelles est essentielle pour se conformer aux réglementations et protéger les individus contre le vol ou l'utilisation abusive d'identité.

Informatique en périphérie : architecture informatique distribuée dans laquelle la puissance de traitement, le stockage et l'analyse des données sont situés plus près de l'endroit où les données sont générées (sur des appareils, des passerelles ou des serveurs « périphériques » locaux) plutôt que centralisés dans des centres de données cloud distants. Cette approche améliore le temps de réponse, réduit la latence et l'utilisation de la bande passante, et permet des applications en temps réel ou quasi réel, en particulier dans les objets connectés, les systèmes autonomes et les environnements où la rapidité ou la prise de décision locale sont importantes.

Infrastructure en tant que service (Infrastructure-as-a-Service /IaaS) : modèle de cloud qui fournit des ressources informatiques virtualisées, telles que des serveurs, du stockage et des réseaux, via Internet sur la base d'un paiement à l'utilisation. L'IaaS permet aux entreprises de faire évoluer rapidement leur infrastructure sans investir dans du matériel physique, tout en garantissant la flexibilité, la rentabilité et un déploiement rapide.

Ingénierie de prompts : pratique qui consiste à élaborer, affiner et optimiser des instructions d'entrée (les prompts) afin d'orienter un modèle d'IA génératif vers la production de résultats précis, pertinents et utiles. Une ingénierie de prompts efficace améliore l'efficacité, la cohérence et la fiabilité des systèmes d'IA, leur permettant d'effectuer des tâches telles que le résumé, la traduction, le codage ou la génération créative avec une qualité supérieure. À mesure que les modèles d'IA gagnent en capacité, l'ingénierie rapide est devenue une discipline clé pour aligner les résultats sur les intentions des utilisateurs et les objectifs commerciaux.

Intelligence artificielle : technologie qui permet aux machines ou aux logiciels d'exécuter des tâches qui nécessitent normalement l'intelligence humaine, comme l'apprentissage, le raisonnement, la perception, la résolution de problèmes, la prise de décision, la compréhension du langage naturel et la reconnaissance de modèles. Les systèmes d'IA imitent ou simulent les fonctions cognitives de l'esprit humain en utilisant des algorithmes, des volumes importants de données et une puissance de calcul. Comme l'IA englobe une grande variété de méthodes (de l'apprentissage automatique aux réseaux neuronaux et à l'apprentissage profond), ses applications peuvent aller de l'analyse de la parole et du texte à la réalisation de prédictions, en passant par la traduction de langues, générer du contenu créatif ou optimiser des processus complexes.

Intelligence artificielle agentique : IA agentique désigne le cadre des systèmes d'intelligence artificielle conçus pour fonctionner comme des agents autonomes. Contrairement aux modèles qui répondent simplement à une demande, un agent peut percevoir son environnement, créer un plan en plusieurs étapes, prendre des décisions indépendantes et utiliser des outils pour travailler activement à la réalisation d'un objectif spécifique.

Dans un contexte d'entreprise, ces agents constituent un puissant moteur de productivité, les données servant de carburant. Ils peuvent avoir accès à des ensembles de données d'entreprises privées et à des outils internes, ce qui leur permet d'automatiser des flux de traitement complexes qui nécessitaient auparavant un jugement humain. L'IA agentique fonctionne avec un « cerveau numérique », un modèle unique et compétent capable de traiter des décennies de réponses humaines.

Intelligence artificielle étroite (IAE) : désigne les systèmes d'IA conçus et entraînés pour effectuer des tâches spécifiques ou résoudre des problèmes définis, souvent au niveau ou au-dessus des capacités humaines, mais sans capacité générale de raisonnement ou de compréhension au-delà de leur domaine de programmation.

Intelligence artificielle générale (IAG) : une IAG représente une intelligence avancée capable de redéfinir non seulement des secteurs, mais aussi des sociétés entières. Cela fait référence à une IA qui possède la capacité de comprendre, d'apprendre et d'appliquer des connaissances dans un large éventail de tâches, un peu comme un être humain. Malgré ses vastes capacités, une IAG est toujours façonnée par la qualité et l'apport de ses données d'entraînement.

Intelligence Artificielle Supérieure (IAS) : forme hypothétique d'IA qui surpasse l'intelligence humaine dans tous les domaines, y compris le raisonnement, la créativité, la compréhension sociale et la prise de décision stratégique, et qui serait capable de surpasser les meilleurs esprits humains dans tous les domaines.

Intelligence commerciale (IC) : technologies, outils et pratiques qui collectent, intègrent et analysent les données commerciales pour faciliter la prise de décision. Les plateformes d'IC transforment les données brutes en tableaux de bord, rapports et visualisations, aidant ainsi les entreprises à identifier les tendances, à mesurer les performances et à faire des choix stratégiques plus éclairés.

Intelligence contextuelle : capacité des systèmes, des organisations ou des individus à interpréter des données, des événements ou des comportements dans le contexte qui les entoure et à agir de manière appropriée. Dans le domaine de la technologie, cela fait référence à l'utilisation par l'IA de signaux en temps réel, tels que la localisation, le comportement, les préférences ou le moment, pour fournir des analyses, des recommandations et des actions plus pertinentes. Dans les médias et le marketing, l'intelligence contextuelle favorise la personnalisation et l'orchestration du parcours client en garantissant que chaque interaction est opportune, significative et alignée sur les besoins des clients.

Interface de programmation d'applications (API) : ensemble de règles et de protocoles logiciels permettant à deux applications de communiquer entre elles. Les API fournissent aux systèmes d'IA un moyen structuré de se connecter par programmation à des modèles externes, à des ensembles de données ou à d'autres composants logiciels.

Interface utilisateur graphique (GUI) : interface visuelle qui permet aux utilisateurs d'interagir avec des logiciels ou des appareils par le biais d'éléments graphiques tels que des fenêtres, des icônes, des boutons et des menus, plutôt que par la saisie de commandes textuelles. Les interfaces graphiques rendent la technologie plus intuitive et plus accessible en permettant la navigation par pointer-cliquer, les actions glisser-déposer et le retour visuel.

Internet des objets (IdO/IoT) : désigne un réseau d'appareils physiques, tels que des capteurs, des appareils, des véhicules et des machines, connectés à Internet et capables de collecter, de partager et d'agir sur des données, permettant ainsi l'automatisation, la personnalisation et une prise de décision plus intelligente en temps réel.

Interopérabilité : capacité des différents systèmes, applications ou plateformes à échanger et à utiliser des données de manière fluide. En s'appuyant sur des normes et des protocoles communs, l'interopérabilité réduit les obstacles techniques et permet à divers systèmes de fonctionner ensemble efficacement.

Kubernetes : plateforme open source (gratuite) permettant d'automatiser le déploiement, le dimensionnement et la gestion des applications conteneurisées. Développé à l'origine par Google, Kubernetes orchestre des groupes (clusters) de conteneurs (gestion de la planification, de l'équilibrage de charge et de la reprise après incident afin que les applications s'exécutent de manière fiable et efficace dans le cloud, sur site ou en environnements hybrides.

Lac de données (Data Lake) : référentiel de stockage centralisé qui contient de grandes quantités de données brutes dans leur format natif, qu'elles soient structurées, semi-structurées ou non structurées. Contrairement aux bases de données ou aux entrepôts de données traditionnels, les lacs de données permettent aux entreprises de stocker les données dans un premier temps et de les organiser ou de les er ultérieurement, en prenant en charge l'e des mégadonnées, l'apprentissage automatique et les informations en temps réel.

Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) : Loi fédérale canadienne sur la protection des renseignements personnels régissant la façon dont les organisations du secteur privé recueillent, utilisent et divulguent les renseignements personnels dans le cadre des activités commerciales. La LPRPDE accorde aux individus le droit d'accéder à leurs données et de les corriger, oblige les organisations à obtenir un consentement éclairé et impose des mesures de protection pour protéger les informations personnelles.

Main-d'œuvre numérique : ensemble de systèmes logiciels automatisés, appelés « travailleurs numériques » (tels que les agents d'intelligence artificielle, robots et assistants virtuels), qui exécutent des tâches traditionnellement effectuées par des humains.

Métadonnées : ensemble de termes, de mots, de symboles et de chiffres intégrés dans un document pour permettre des fonctions de gestion des dossiers telles que la classification, la recherche, le suivi historique (date de création, de modification, de récupération), l'identification des utilisateurs (auteurs et éditeurs des modifications), et une variété d'autres éléments liés à ses caractéristiques.

Microservices : approche architecturale du développement logiciel dans laquelle les applications sont structurées comme un ensemble de petits services indépendants communiquant via des API. Chaque microservice se concentre sur une fonction commerciale spécifique, peut être développé et déployé indépendamment, et évolue séparément. Cette conception améliore la flexibilité, la résilience et la maintenabilité par rapport aux architectures monolithiques.

Modernisation (logicielle) : processus plus large de mise à jour des systèmes, applications ou infrastructures existants afin de tirer parti des technologies, architectures et pratiques modernes. Alors que la migration se concentre souvent sur la relocalisation des systèmes existants, la modernisation peut impliquer une refonte, une refonte de la plateforme ou une reconception afin d'améliorer l'évolutivité, l'agilité et la valeur commerciale à long terme.

Modèle multirégional : architecture cloud dans laquelle les applications et les données sont déployées dans plusieurs régions géographiques proposées par un fournisseur cloud. Ce modèle améliore la disponibilité, les performances et la reprise après sinistre en répartissant les charges de travail au plus près des utilisateurs finaux et en garantissant la redondance en cas de panne ou de latence dans une région.

Modèles linguistiques étendus (MLE) : type de modèle de base basé sur l'apprentissage profond, préformé sur d'énormes corpus de textes à l'aide de méthodes autosupervisées. Ces modèles traitent les entrées sous forme de « jetons » (morceaux de mots ou de caractères), apprennent les relations statistiques entre elles et utilisent ces relations pour comprendre, générer, résumer ou transformer un texte en langage humain. En raison de leur taille et de leur architecture (souvent basées sur des transformateurs), les MLE peuvent effectuer de nombreuses tâches linguistiques « prêtes à l'emploi », mais peuvent également être affinées ou guidées par une ingénierie rapide pour des applications spécifiques. Les modèles GPT-4 et Llama de Meta sont des exemples de MLE.

Modèle de confiance zéro/Zero-Trust : cadre de sécurité qui suppose qu'aucun utilisateur, appareil ou système ne doit être approuvé par défaut, que ce soit à l'intérieur ou à l'extérieur du réseau d'une entreprise. En informatique, la confiance zéro (Zero Trust) nécessite une vérification continue de l'identité, des contrôles d'accès stricts et une surveillance de toutes les activités afin de minimiser les risques et de protéger les données sensibles.

Modèles fondamentaux : de grands modèles d'apprentissage profond entraînés sur d'énormes quantités de données non structurées et non étiquetées, conçus pour effectuer une grande variété de tâches directement ou en les adaptant à des applications spécifiques. Les modèles de base peuvent également être utilisés à des fins génératives ou non génératives (par exemple, pour classer le sentiment des utilisateurs comme négatif ou positif sur la base des transcriptions d'appels).

Moteurs de recommandation : systèmes logiciels qui analysent les données et le comportement des utilisateurs pour suggérer des produits, des services ou du contenu pertinents. En informatique, les moteurs de recommandation utilisent des techniques telles que l'apprentissage automatique, le filtrage collaboratif ou le filtrage basé sur le contenu pour personnaliser les expériences utilisateur, comme c'est souvent le cas dans le commerce électronique, les plateformes de streaming et la publication numérique.

Moteur de règles : système qui prend des décisions et applique une logique aux flux de traitement en fonction de règles métier prédéfinies.

Multi-cloud : stratégie cloud dans laquelle une organisation utilise les services de deux ou plusieurs fournisseurs cloud simultanément. Cette approche permet de réduire la dépendance vis-à-vis des fournisseurs, d'accroître la résilience, d'optimiser les performances et de répondre aux exigences réglementaires ou géographiques en répartissant les charges de travail sur plusieurs plateformes telles qu'AWS, Microsoft Azure et Google Cloud.

Multivers : système complexe dans lequel coexistent plusieurs modèles commerciaux, formats de contenu et sources de revenus interconnectés.

Opérations d'apprentissage automatique (MLops) : cadre rigoureux pour gérer le cycle de vie de bout en bout des modèles d'apprentissage automatique en production. MLops intègre les principes DevOps à l'IA, garantissant que les modèles sont développés, déployés, surveillés et gouvernés de manière fiable à grande échelle. Il englobe les pipelines de données, la création de versions des modèles, le suivi des performances, la détection des biais et des dérives, les contrôles de sécurité et l'auditabilité. L'objectif de MLOps est d'opérationnaliser l'IA de manière responsable - en fournissant des résultats cohérents, en réduisant les risques et en activant l'amélioration continue dans les systèmes de l'entreprise.

Opérations sur les modèles linguistiques étendus (LLMOps) : extension spécialisée de MLops axée sur les exigences uniques en matière de cycle de vie des grands modèles linguistiques. Les LLMops gèrent la manière dont les modèles de base sont sélectionnés, affinés, déployés, surveillés et gouvernés, y compris la gestion rapide, les contrôles de sécurité, la gouvernance des accès, la réduction des hallucinations et la rentabilité. Ils garantissent que les MLE fonctionnent en toute sécurité avec les données de l'entreprise, respectent les exigences politiques et réglementaires et fournissent des performances fiables. Dans l'entreprise, les LLMops sont essentiels pour faire évoluer l'IA générative de manière responsable tout en protégeant l'intégrité et la confiance des données.

Orchestrateur : système, outil ou humain qui coordonne et gère plusieurs composants ou processus afin qu'ils travaillent ensemble pour exécuter des tâches complexes. (Voir également : Routeur de requêtes pour les données souveraines/contexte IA).

Outils d'analyse des sentiments : applications logicielles qui utilisent le traitement du langage naturel, l'apprentissage automatique ou des méthodes statistiques pour identifier et catégoriser les opinions ou les émotions exprimées sous forme de texte, de discours ou d'autres données. Ces outils aident les organisations à déterminer si le sentiment est positif, négatif ou neutre. Ils sont couramment utilisés dans des domaines tels que les commentaires clients, la surveillance des réseaux sociaux et les études de marché.

Pistes d'audit : enregistrements chronologiques qui suivent les activités du système, y compris les actions des utilisateurs, les modifications des données et les événements d'accès. Ces traces assurent la transparence, soutiennent le respect des réglementations et facilitent les enquêtes de sécurité en indiquant qui a fait quoi, quand et comment au sein d'un système.

Plateforme : environnement informatique qui fournit l'infrastructure, les logiciels et les outils sous-jacents nécessaires à l'exécution des applications ou des services. Les plateformes peuvent inclure des systèmes d'exploitation, des environnements cloud ou des environnements de développement d'applications qui prennent en charge le développement, le déploiement et l'intégration. Elles constituent la base sur laquelle les utilisateurs, les développeurs ou les organisations créent et gèrent des solutions numériques.

Plateforme en tant que service (PaaS) : modèle informatique cloud qui fournit aux développeurs une plateforme prête à l'emploi, comprenant une infrastructure, des systèmes d'exploitation et des outils de développement, pour créer, tester et déployer des applications. Une PaaS fait abstraction de la gestion du matériel et du système, permettant aux équipes de se concentrer sur le codage et l'innovation tout en garantissant l'évolutivité, la sécurité et l'intégration avec d'autres services cloud.

Plateforme/Ensemble de technologies compatibles avec l'IA : environnement technologique conçu pour héberger et intégrer le développement, le déploiement, y compris à grande échelle, d'applications d'intelligence artificielle. Il combine une infrastructure évolutive, une solide gouvernance des données et des outils modulaires, tels que les API, la gestion des modèles et les connecteurs, pour délivrer plus rapidement les projets d'IA et les rendre, plus fiables et plus faciles à faire passer de l'expérimentation à la production.

Plateformes héritées : systèmes technologiques, logiciels ou infrastructures obsolètes ou anciens qui restent utilisés malgré leur remplacement par de nouvelles alternatives. Les plateformes existantes peuvent toujours prendre en charge les opérations commerciales critiques, mais présentent souvent des défis tels qu'une compatibilité limitée, des coûts de maintenance plus élevés, des failles de sécurité et des difficultés d'intégration aux solutions modernes.

Planification des ressources de l'entreprise (PRE) : système logiciel intégré qui gère les principaux processus de l'entreprise - tels que la finance, la chaîne d'approvisionnement, la fabrication, les ressources humaines et les relations avec les clients - dans une plateforme unifiée. La PRE centralise les données et les flux de traitement entre les départements, améliorant ainsi l'efficacité, la collaboration et la prise de décision tout en fournissant une source unique de vérité pour l'organisation.

Reconnaissance optique de caractères (OCR) : technologie qui convertit du texte imprimé ou manuscrit dans des documents ou des images numérisés en texte numérique lisible par machine, permettant ainsi la recherche, l'édition et l'automatisation du traitement.

Référentiel : emplacement de stockage, souvent géré à l'aide d'outils tels que GitHub ou GitLab, où sont conservés une base de code et son historique des modifications. Alors que la base de code fait référence au code lui-même, le référentiel suit également les révisions, les branches et les contributions, ce qui permet aux équipes de gérer le code et de collaborer efficacement sur le code.

Règlement général sur la protection des données (RGPD) : loi importante sur la confidentialité et la protection des données promulguée par l'Union européenne en 2018. Le RGPD régit la manière dont les organisations collectent, traitent, stockent et partagent les données personnelles, en mettant l'accent sur la transparence, le consentement des utilisateurs et les droits individuels, avec des sanctions importantes en cas de non-conformité.

Résidence des données : emplacement physique ou géographique où les données d'une organisation sont stockées et traitées. Souvent dictée par des exigences légales, réglementaires ou commerciales, la résidence des données garantit que les informations restent dans des juridictions spécifiques, ce qui peut avoir un impact sur la conformité, la sécurité et les performances.

Retour sur investissement (RSI Return On Investment/ROI) : indicateur de performance qui mesure la rentabilité ou l'efficacité d'un investissement, calculé en comparant le gain ou l'avantage net à son coût. Dans les contextes informatiques et commerciaux, le retour sur investissement est utilisé pour évaluer la valeur des initiatives technologiques, des projets ou des achats en quantifiant les rendements financiers par rapport aux ressources investies.

Routeur de requêtes : fonction intelligente qui utilise un moteur de règles pour déterminer comment acheminer les données souveraines et non souveraines en fonction de la demande d'un flux de traitement d'intelligence artificielle agentique.

Sécurité des données : ensemble de pratiques, de technologies et de politiques utilisées pour protéger les informations numériques contre tout accès non autorisé, toute corruption ou toute perte. Il comprend des mesures telles que le chiffrement, les contrôles d'accès, les sauvegardes et la surveillance afin de préserver la confidentialité, l'intégrité et la disponibilité des données tout au long de leur cycle de vie. (Voir également : Cybersécurité, Conformité, Confidentialité des données).

Services gérés : opérations et responsabilités informatiques externalisées fournies par un fournisseur de services tiers. Dans le domaine de l'informatique, les services gérés incluent généralement la surveillance proactive, la maintenance, la sécurité, les mises à jour et le support de l'infrastructure, des applications ou des environnements cloud. Cette approche permet aux organisations de réduire la charge de travail des équipes internes, de garantir la fiabilité du système et d'accéder à une expertise spécialisée tout en se concentrant sur les activités commerciales de base.

Silos de données : ensembles de données isolés qui sont contrôlés par un service, un système ou une plateforme et qui ne sont pas facilement accessibles aux autres membres d'une organisation. Les silos de données limitent la collaboration, réduisent la visibilité et peuvent créer des inefficiences ou des incohérences, rendant ainsi plus difficile l'obtention d'une vue unifiée des informations à l'échelle de l'entreprise. Souveraineté des données : principe selon lequel les données numériques sont soumises aux lois et aux structures de gouvernance du pays ou de la région où elles sont collectées, stockées ou traitées. Il garantit que le traitement des données est conforme aux réglementations locales, telles que le RGPD dans l'UE ou les lois sur la localisation des données ailleurs, qui affectent la manière dont les entreprises gèrent le stockage, la sécurité et les transferts transfrontaliers.

Souveraineté des données : principe selon lequel les données numériques sont soumises aux lois et aux structures de gouvernance du pays ou de la région où elles sont collectées, stockées ou traitées. Il garantit que le traitement des données est conforme aux réglementations locales, telles que le RGPD dans l'UE ou les lois sur la localisation des données ailleurs, qui affectent la manière dont les entreprises gèrent le stockage, la sécurité et les transferts transfrontaliers.

Système de gestion de contenu (Content Management System/CMS) : plateforme logicielle qui permet aux utilisateurs de créer, de modifier, d'organiser et de publier du contenu numérique, généralement pour des sites Web, sans avoir besoin de compétences techniques approfondies. Les plateformes CMS telles que WordPress, Drupal ou Adobe Experience Manager fournissent des modèles, des flux de traitement et des intégrations qui rendent la gestion du contenu en ligne plus efficace et collaborative. Un CMS gère le contenu du site Web à des fins de publication, tandis qu'un système de gestion de contenu d'entreprise (GCE) gère toutes les informations organisationnelles tout au long de leur cycle de vie à des fins de gouvernance, de conformité et de processus commerciaux.

Traitement du langage naturel (TLN) : domaine de l'intelligence artificielle qui permet aux ordinateurs de comprendre, d'interpréter et de générer le langage humain. Le TLN combine la linguistique, l'apprentissage automatique et les techniques informatiques pour prendre en charge des applications telles que les chatbots, la traduction, l'analyse des sentiments et la reconnaissance vocale.

Visionnaire : un visionnaire fait référence à une personne qui se projette dans l'avenir pour prendre des décisions proactives. Ces personnes minimisent les risques associés aux événements et aux résultats potentiels. Un visionnaire apportera les modifications nécessaires à l'avance ou créera des protocoles qui pourront être mis en œuvre en cas de besoin. Il est prêt à faire face à presque tout.

Études citées

Agrawal, A., Gans, J., and Goldfarb, A. "Prediction Machines: The Simple Economics of Artificial Intelligence." *Harvard Business Review Press*, 2022.

"AI Governance Framework: Transparency, Explainability, and Contestability (TEC)." *AI-Governance.eu*, 2024. https://ai-governance.eu/ai-governance-framework/tec/. (Consulté en octobre 2025).

"AI Governance Software Spend Will See 30% CAGR From 2024 to 2030." *Blog Forrester*, 13 novembre 2024. www.forrester.com/blogs/ai-governance-software-spend-will-see-30-cagr-from-2024-to-2030/. (Consulté en octobre 2025).

Barrenechea, Mark J. and Tom Jenkins. *Digital Financial Services*. OpenText Corporation, 2016. Barrenechea, Mark J. and Tom Jenkins. Digital Manufacturing. OpenText Corporation, 2018.

Barrenechea, Mark J. and Tom Jenkins. *e-Government or Out of Government*. OpenText Corporation, 2014.

Barrenechea, Mark J. and Tom Jenkins. *Enterprise Information Management: The Next Generation of Enterprise Software*. OpenText Corporation, 2013.

Barrenechea, Mark J., Jenkins, Tom, and David Fraser. *The Anticipant Organization*. OpenText Corporation, 2022.

Biggio, B., Nelson, B. and P. Laskov. "Poisoning Attacks Against Support Vector Machines." *Proceedings of the 29th International Conference on Machine Learning (ICML)*, 2012.

Boyd, K. "Microsoft 365 copilot for executives: Sharing Our Customer Zero Deployment and adoption journey at Microsoft." *Blog Microsoft Inside Track*, 5 décembre 2024. https://www.microsoft.com/insidetrack/blog/copilot-for-microsoft-365-for-executives-sharing-our-internal-deployment-and-adoption-journey-at-microsoft/. (Consulté en octobre 2025).

Bubeck, Sébastien, Chandrasekaran, Varun, Eldan Ronen et al. "Sparks of artificial general intelligence: Early experiments with GPT-4." *Université Cornell*, arXiv:2303.12712, 13 avril 2023. https://arxiv.org/abs/2303.12712. (Consulté en octobre 2025).

Challapally, Aditya, Pease, Chris, Raskar, Ramesh et al. "The GenAI Divide: The State of AI in Business 2025." *Rapport NANDA du MIT*. École de gestion Sloan du MIT, juillet 2025. https://mlq.ai/media/quarterly_decks/v0.1_State_of_AI_in_Business_2025_Report.pdf. Consulté en octobre 2025).

Crévier, Daniel. *AI: The tumultuous history of the search for artificial intelligence*. Livres de base, 1993.

"Cyber Risks Associated with Generative Artificial Intelligence." *Monetary Authority of Singapore (MAS), Circular No.* TRPD-G01-2024, août 2024, August 2024. https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/cyber-risks-associated-with-generative-artificial-intelligence.pdf. (Consulté en octobre 2025).

Daugherty, Paul, Ghosh, Bhaskar, Narain, Karthik, et al. "A new generative era of AI for everyone." *Accenture*, 2023.

"Data Sovereignty as Your Foundation Layer." *Katonic Blog*, 13 octobre 2025. https://www.katonic.ai/blog/building-your-ai-stack-data-sovereignty-as-your-foundation-layer. (Consulté en octobre 2025).

"Deepfake and AI Phishing Statistics (2024)." *ZeroThreat.ai*. ZeroThreat, 2024. https://zerothreat.ai/blog/deepfake-and-ai-phishing-statistics. (Consulté en octobre 2025).

Edquist, Alex, Grennan, Liz, Griffiths, Sian et al. “Data ethics: What it means and what it takes.” *McKinsey & Company*, 23 septembre 2022. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/data-ethics-what-it-means-and-what-it-takes. (Consulté en octobre 2025).

Commission européenne. Règlement (UE) 2024/1689 sur l’intelligence artificielle, 2024.

Parlement européen et Conseil. « Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données personnelles. » *Article 17* (Droit à l’effacement), 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj. (Consulté en octobre 2025).

Cooper, A. Feder, Choquette-Choo, Christopher A., Bogen, Miranda et al. “Machine Unlearning Doesn’t Do What You Think: Lessons for Generative AI Policy, Research, and Practice.” *SSRN*, 6 février 2025. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5060253. (Consulté en octobre 2025).

Foundry Research commandité par OpenText. “MarketPulse Survey: The Role of GenAI in Modernizing Content Management.” Mai 2025.

“Gartner Poll Finds 55% of Organizations Have an AI Board.” Gartner, Inc. Press Release, 26 juin 2024.

“Gartner Says More Than 80% of Enterprises Will Have Used Generative AI APIs or Deployed Generative AI-Enabled Applications by 2026.” *Gartner Inc. Press Release.*, 11 octobre 2023. www.gartner.com/en/newsroom/press-releases/2023-10-11-gartner-says-more-than-80-percent-of-enterprises-will-have-used-generative-ai-apis-or-deployed-generative-ai-enabled-applications-by-2026. (Consulté en octobre 2025).

“Gartner Survey Reveals GenAI Attacks Are on the Rise.” *Gartner Inc.,* 22 semptembre 2025. https://www.gartner.com/en/newsroom/press-releases/2025-09-22-gartner-survey-reveals-generative-artificial-intelligence-attacks-are-on-the-rise. (Consulté en octobre 2025).

Goodfellow, Ian J., Shlens, Jonathon and Christian Szegedy. “Explaining and Harnessing Adversarial Examples.” *Université Cornell*, arXiv:1412.6572, 20 mars 2015. https://arxiv.org/abs/1412.6572. (Consulté en octobre 2025).

“The Artificial Intelligence Pathway to the Future of Work.” *Forrester Research*, juin 2023..

Gu, Tianyu, Dolan-Gavitt, Brendan and Siddharth Garg. “BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain.” *Université Cornel*, arXiv:1708.06733, 11 mars 2019. https://arxiv.org/abs/1708.06733. (Consulté en octobre 2025).

Hintze, Arend. “Understanding the four types of AI, from reactive robots to self-aware beings.” The Conversation, 13 novembre 2016. https://theconversation.com/understanding-the-four-types-of-ai-from-reactive-robots-to-self-aware-beings-67616. (Consulté en octobre 2025).

“How we built our multi-agent research system.” *Anthropic*, 2024. https://www.anthropic.com/engineering/multi-agent-research-system. (Consulté en octobre 2025).

“Information Governance Reference Model.” EDRM. http://www.edrm.net/projects/igrm. (Consulté en octobre 2025).

Organization for Standardization. “Artificial Intelligence Standards Portfolio.” ISO/CEI JTC 1/SC 42, 2023.

International Organization for Standardization. “Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements.” ISO/IEC 27001:2022.

International Organization for Standardization. “What is Artificial Intelligence (AI)?” 31 janvier 2024. https://www.iso.org/artificial-intelligence/what-is-ai?. (Consulté en octobre 2025).

Jangam, Sandeep Kumar. “Importance of Encrypting Data in Transit and at Rest Using TLS and Other Security Protocols and API Security Best Practices.” *International Journal of AI*, BigData, *Computational and Management Studies*, 4 (3), 82—91, 2023. https://ijaibdcms.org/index.php/ijaibdcms/article/view/242/. (Consulté en octobre 2025).

Jenkins, Tom. *Behind the firewall: Big Data and the Hidden Web: The Path to Enterprise Information Management.* OpenText Corporation, 2012.

Jenkins, Tom. *Enterprise Content Management: What You Need to Know.* OpenText Corporation, 2004.

Jenkins, Tom. *Managing Content in the Cloud: Enterprise Content Management 2.0.* OpenText Corporation, 2011.

Jiang, Shuli, Kadhe, Swanand Ravindra, Zhou, Yi et al. "Forcing Generative Models to Degenerate Ones: The Power of Data Poisoning Attacks." *Université Cornell*, arXiv:2312.04748, 7 décembre 2023. https://arxiv.org/abs/2312.04748. (Consulté en octobre 2025).

Joshi, Akshay, Moschetta, Giulia and Ellie Winslow. "Global Cybersecurity Outlook 2025 Insight Report." *World Economic Forum in Collaboration with Accenture*, janvier 2025. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf. (Consulté en octobre 2025).

Kandogan, Eser, Bhutani, Nikita, Zhang, Dan et al. "Orchestrating Agents and Data for Enterprise: A Blueprint Architecture for Compound AI." *arXiv Preprint*, 10 avril 2025. https://arxiv.org/abs/2504.08148. (Consulté en octobre 2025).

Kaplan, Jared, McCandlish, Sam, Henighan, Tom et al. "Scaling Laws for Neural Language Models." Cornell Université, arXiv:2001.08361, 23 janvier 2020. https://arxiv.org/abs/2001.08361. (Consulté en octobre 2025).

"Key Regulatory and Industry Initiatives." Capgemini https://web.archive.org/web/20141105171058/https://www.worldpaymentsreport.com/kriis#Heat-Map-of-KRIIs-Global-and-Regional. (Consulté en octobre 2025).

"Key Terms for AI Governance." *International Association of Privacy Professionals (IAPP)*, 2024. https://iapp.org/resources/article/key-terms-for-ai-governance/. (Consulté en octobre 2025).

Kourinian, Arsen and Mayer Brown. "Addressing Transparency & Explainability When Using AI Under Global Standards." *Bloomberg Law*, 2024. https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2024/01/addressing-transparency-and-explainability-when-using-ai-under-global-standards.pdf. (Consulté en octobre 2025).

Kurakin, Alexey, Goodfellow, Ian and Samy Bengio. "Adversarial Machine Learning at Scale." *Cornell University*, arXiv:1611.01236, 11 février 2017. https://arxiv.org/abs/1611.01236. (Consulté en octobre 2025).

LeCun Yann, Bengio, Yoshua, and Geoffrey Hinton. "Deep learning." *Nature*, 521 (7553), 436—444, 2015. https://doi.org/10.1038/nature14539, (Consulté en octobre 2025).

Lu, Ruei-Shan, Lin, Ching-Chang and Hsiu-Yuan Tsao. "Empowering Large Language Models to Leverage Domain-Specific Knowledge in E-Learning." *Applied Sciences*, 14 (12), 5264, 18 juin 2024. https://doi.org/10.3390/app14125264. (Consulté en octobre 2025).

Lutkevich, Ben. "What is AI Winter? Definition, History and Timeline." Tech Target, 26 août 2024. https://www.techtarget.com/searchenterpriseai/definition/AI-winter. (Consulté en octobre 2025).

Marcus, Gary. "Deep learning is hitting a wall." *Communications of the ACM*, 65 (8), 36-43, 2022. https://nautil.us/deep-learning-is-hitting-a-wall-238440/. (Consulté en octobre 2025).

Maisto, Dario. "From Digital Sovereignty Platforms To Sovereign Cloud Platforms: Three Reasons For A Title Change." *Forrester Blogs*, 11 août 2025. www.forrester.com/blogs/from-digital-sovereignty-platforms-to-sovereign-cloud-platforms-three-reasons-for-a-title-change/. (Consulté en octobre 2025).

McCarthy, J., Minsky, M. L., Rochester N. et al. "A proposal for the Dartmouth summer research project on artificial intelligence." *Dartmouth College*, 1955. https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/1904. (Consulté en octobre 2025).

Mienye, I.D., Jere, N., Obaido, G. et al. “Large language models: an overview of foundational architectures, recent trends, and a new taxonomy.” *Discov Appl Sci 7*, 1027, 2025. https://doi.org/10.1007/s42452-025-07668-w. (Consulté en octobre 2025).

McKinsey & Company. “Future-Proofing the IT Function Amid Global Trends and Disruptions.” *McKinsey Digital*, 11 juin 2025. www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/future-proofing-the-it-function-amid-global-trends-and-disruptions. (Consulté en octobre 2025).

McKinsey & Company. “The State of AI in Early 2024: Gen AI Adoption Spikes and Starts to Generate Value.” *QuantumBlack by McKinsey*, 30 mai 2024. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-2024. (Consulté en octobre 2025).

Mehrabi, Ninareh, Morstatter, Fred, Saxena, Nripsuta et al. “A Survey on Bias and Fairness in Machine Learning.” *Cornell University*, arXiv : 1908.09635, 25 janvier 2022. https://arxiv.org/abs/1908.09635. (Consulté en octobre 2025).

Mei, Lingrui, Yao, Jiayu, Ge Yuyao et al. “A survey of context engineering for large language models.” *Cornell University*, arXiv:2507.13334, 21 juillet 2025. https://arxiv.org/abs/2507.13334. (Consulté en octobre 2025).

Miller, Philip. “Unlocking Unstructured Data: Fueling AI with Insights.” *Dataversity*, 3 juin 2025. https://www.dataversity.net/articles/unlocking-unstructured-data-fueling-ai-with-insights/. (Consulté en octobre 2025).

Moor, James. “What is Computer Ethics?” *Metaphilosophy,* 16 (4), 266—275, 1985, https://doi.org/10.1111/j.1467-9973.1985.tb00173.x. (Consulté en octobre 2025).

“More Than 80% of Enterprises Will Have Used Generative AI APIs or Deployed Generative AI Applications by 2026.” *Gartner Inc. Press Release*, October 11, 2023. www.gartner.com/en/newsroom/press-releases/2023-10-11-gartner-says-more-than-80-percent-of-enterprises-will-have-used-generative-ai-apis-or-deployed-generative-ai-enabled-applications-by-2026. (Consulté en octobre 2025).

Mucci, Tim and Cole Stryker. “What is artificial superintelligence?” IBM, 22 juillet 2025. https://www.ibm.com/think/topics/artificial-superintelligence. (Consulté en octobre 2025).

“New Accenture Research Finds that Companies with AI-Led Processes Outperform Peers.” Accenture, 10 octobre 2024. https://newsroom.accenture.com/news/2024/new-accenture-research-finds-that-companies-with-ai-led-processes-outperform-peers. (Consulté en octobre 2025).

NIST. “Artificial Intelligence Risk Management Framework (AI RMF 1.0).” *NIST Special Publication AI 100-1*, 2023.

Organisation for Economic Co-operation and Development. “Recommendation of the Council on Artificial Intelligence.” *OECD/LEGAL/0449*, 2019.

O’Grady, Michael, and Michele Goetz, et al. “Global Commercial AI Software Governance Market Forecast, 2024 to 2030.” *Forrester Research*, 1 novembre 2024.

“Predicts 2025: Data and Analytics Strategy—Unlocking Value with AI and Governance.” *Gartner Inc.*, 2024.

Propriétaire du produit. *Scaled Agile Framework*, 25 février 2025. https://framework.scaledagile.com/product-owner. (Consulté en octobre 2025).

Rabot, M. “Winning in the Autonomous AI Agents Race.” *Medium*, 4 avril 2025 https://rabot.medium.com/winning-in-the-autonomous-ai-agents-race-a0c03d52acad. (Consulté en octobre 2025).

Rose, Scott, Borchert, Oliver, Mitchell, Stu et al. “Zero Trust Architecture.” NIST Special Publication 800-207, août 2020. https://doi.org/10.6028/NIST.SP.800-207. (Consulté en octobre 2025).

Rowe, Adam. “MIT finds 95% of Enterprise AI Pilots Fail to Deliver Revenues, *Tech.co*, 20 août 2025. https://tech.co/news/mit-enterprise-ai-pilots-fail-revenues. (Consulté en octobre 2025).

Russell, Melissa. “How can I learn artificial intelligence?” *Harvard*, le 8 avril 2025. https://extension.harvard.edu/blog/how-can-i-learn-artificial-intelligence/#What-is-Artificial-Intelligence. (Consulté en octobre 2025).

Russell, S.J. and P. Norvig. Artificial intelligence: A modern approach. 4th ed., *Pearson*, 2021.

Sanchez, Jarvy. “Enterprise AI Architecture | Components & Best Practices.” *Leanware*, 28 août 2025. https://www.leanware.co/insights/enterprise-ai-architecture. (Consulté en octobre 2025).

Samoili, S., López Cobo, M., Delipetrev, B. et al. “AI Watch, Defining Artificial Intelligence 2.0: Towards an operational definition and taxonomy for the AI Landscape.” *Publications Office of the European Union*, 2021.

Semba, Kurt. “Artificial Intelligence, Real Consequences: Confronting AI’s Growing Energy Appetite.” *Extreme Networks*, 15 août 2024. https://www.extremenetworks.com/resources/blogs/confronting-ai-growing-energy-appetite-part-1. (Consulté en octobre 2025).

Singla, Alex, Sukharevsky, Alexander, Yee Lareina et al. The State of AI: How Organizations Are Rewiring to Capture Value. *McKinsey & Company*, 2025.

Stanford University. AI Index Report 2025. *Stanford Institute for Human-Centered Artificial Intelligence*, 2025.

Sukharevsky, Alexander, Krivkovich, Alexis, Gast, Arne et al. “The agentic organization: Contours of the next paradigm for the AI era.” *McKinsey & Company*, September 26, 2025. https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-agentic-organization-contours-of-the-next-paradigm-for-the-ai-era#/. (Consulté en octobre 2025).

Sunkara, V.L. “KPIs for AI agents and Generative AI: A rigorous framework for evaluation and Accountability.” *International Journal of Scientific Research and Modern Technology*, 3 (4), 22-29, 2024. https://doi.org/10.38124/ijsrmt.v3i4.572. (Consulté en octobre 2025).

Tegmark, M. Life 3.0: Being human in the age of Artificial Intelligence. Vintage Books, *A Division of Penguin Random House LLC*, 2018.

“The State of AI in Early 2024: Gen AI Adoption Spikes and Starts to Generate Value.” *McKinsey & Company*, 30 mai 2024. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-2024. (Consulté en octobre 2025).

“Towards a Unified Agent with Foundation Models.” *Reddit — r/MachineLearning*, 2024. https://www.reddit.com/r/MachineLearning/comments/155wa2p/r_towards_a_unified_agent_with_foundation_models/. (Consulté en octobre 2025).

Turing, A. M. “Computing Machinery and Intelligence.” *Mind*, Volume LIX, Issue 236, Octobre 1950. https://doi.org/10.1093/mind/lix.236.433. (Consulté en octobre 2025).

Uchida, Yusuke, Nagai, Yuki, Sakazawa, Shigeyuki et al. “Embedding Watermarks into Deep Neural Networks.” *Cornell University*, arXiv:1701.04082, 20 avril 2017. https://arxiv.org/abs/1701.04082. (Consulté en octobre 2025).

Unesco. “Recommendation on the Ethics of Artificial Intelligence.” *UNESCO.org*, 2022. https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence. (Consulté en octobre 2025).

University of Michigan College of Engineering. “Up to 30% of the Power Used to Train AI Is Wasted—Here’s How to Fix It.” *Michigan Engineering News*, 12 novembre 2024. https://news.engin.umich.edu/2024/11/up-to-30-of-the-power-used-to-train-ai-is-wasted-heres-how-to-fix-it/. (Consulté en octobre 2025).

“What is Artificial Intelligence (AI)?” *International Organization for Standardization*, 31 janvier 2024. https://www.iso.org/artificial-intelligence/what-is-ai?

Wharton School of the University of Pennsylvania. “The Hidden Cost of AI: Energy Consumption.” *Knowledge@ Wharton*, 25 avril 2024. https://knowledge.wharton.upenn.edu/article/the-hidden-cost-of-ai-energy-consumption/. (Consulté en octobre 2025).

Yang, Wencheng, Wang, Song, Wu, Di et al. “Deep Learning Model Inversion Attacks and Defenses: A Comprehensive Survey.” *Cornell University*, arXiv:2501.18934, 30 avril 2025. https://arxiv.org/abs/2501.18934. (Consulté en octobre 2025).

Yang, Qiang, Liu, Yang, Chen, Tianjian et al. “Federated Machine Learning: Concept and Applications.” *ACM Digital Library*, 28 janvier 2019. https://dl.acm.org/doi/10.1145/3298981. (Consulté en octobre 2025).

Zhang, Qizheng, Hu, Changran, Upasani, Shubhangi et al. “Agentic Context Engineering: Evolving Contexts for Self-Improving Language Models.” *arXiv preprint arXiv:2510.04618*, 2025. (https://www.arxiv.org/pdf/2510.04618. Consulté en octobre 2025).

Zimmermann, Annette and Danielle Casey. Emerging Tech Impact Radar: Generative AI. *Gartner*, 2025.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

INTELLIGENCE ARTIFICIELLE D'ENTREPRISE: Développer une IA de confiance dans le cloud souverain

Il y a eu des moments dans l'histoire de la technologie où tout a changé en même temps. L'arrivée du Web. L'essor du cloud. La révolution mobile. Chaque vague a transformé le mode d'activité des entreprises, la concurrence entre les industries et la façon dont les gens vivent et travaillent.

Mais aucun de ces changements n'est comparable à l'essor de l'IA à l'ère cognitive, ni en rapidité, ni en ampleur, et certainement pas en conséquence.

L'intelligence artificielle est passée de la périphérie de la stratégie d'entreprise à son centre. Il ne s'agit plus d'une initiative de recherche ou d'un ajout expérimental – c'est le nouveau moteur de la productivité, de l'innovation et de l'avantage concurrentiel.

L'intelligence artificielle d'entreprise : *Développer une IA de confiance dans le cloud souverain* explique pourquoi la prochaine ère d'innovation appartient aux entreprises qui traitent l'information comme leur actif le plus stratégique. En nous appuyant sur des décennies d'expérience dans le domaine de la gestion sécurisée et gouvernée des informations, nous montrons comment les entreprises et les gouvernements peuvent créer une intelligence artificielle non seulement performante, mais également gouvernée et sécurisée.

Des prestataires de clouds aux politiques de données souveraines, ce livre explore comment équilibrer la vitesse avec la responsabilité, l'automatisation avec la responsabilité, et l'intelligence avec l'intégrité. Parce que le succès ne dépend pas de ceux qui construisent les systèmes les plus intelligents, mais de ceux en qui nous pouvons avoir confiance.

L'avenir de l'entreprise est intelligent. L'avenir de l'intelligence est gouverné. Et le travail commence maintenant.

01.26 | 243-FR0119-002