

Bâtir une cyberrésilience avec une sécurité multicouche

Découvrez les mesures dont vous avez
besoin pour prospérer dans un environnement
de menaces en constante évolution



Contenu

Introduction	3
Résumé	4
La sécurité multicouche en bref	5
Pourquoi les entreprises doivent-elles penser cyberrésilience ?	6
La couche de prévention	8
La couche de protection	9
La couche de récupération	10
OpenText Cybersecurity : bâtir une activité cyber-résiliente	11
Exemple d'entreprise : compagnie d'assurance santé	12
Prochaines étapes	13

Introduction

En 2022, près d'un tiers des entreprises de taille moyenne ont été touchées par des infections dues à des logiciels malveillants¹. Pour les grandes PME, ce chiffre a frôlé les 60 %¹. Dans le même temps, le coût moyen d'une violation de données pour les entreprises a augmenté, dépassant les quatre millions de dollars². Cette explosion des menaces se produit dans un contexte de transformation numérique rapide.

En 2023, on estime que les entreprises du monde entier dépenseront plus de 2 000 milliards de dollars en numérisation de leurs flux de travail, de leurs chaînes d'approvisionnement et de leurs interactions avec les clients³. Ces investissements répondent à l'évolution des besoins de l'entreprise, les clients exigeant de plus en plus une expérience client numérique ou hybride.

Néanmoins, cette présence numérique en pleine expansion rend les entreprises plus vulnérables que jamais à la cybercriminalité, alors même que le volume de ces crimes explose. Pour éviter les risques réglementaires, d'atteinte à la réputation et autres, l'entreprise a besoin d'un moyen de se défendre.

La réponse est une défense en profondeur, par le biais d'un système multicouche de cyberrésilience. Une sécurité multicouche réduit la surface d'attaque de l'organisation exposée aux cybercriminels, tout en maximisant la protection contre les accès non autorisés et les violations de données. Elle offre également à l'entreprise la plus grande flexibilité et solidité possible en matière de réponse et de récupération face aux cyber-incidents de toutes sortes.

Dans ce livre numérique, nous expliquons comment une approche multicouche de la sécurité peut donner à votre entreprise un avantage sur les cybercriminels et une longueur d'avance sur le marché. Nous couvrons les technologies dont vous avez besoin pour protéger votre entreprise. Enfin, nous vous expliquons comment les leaders du marché utilisent ces technologies pour protéger votre investissement dans la transformation numérique... et bien plus encore.

1. <https://www.opentextcybersecurity.com/threat-report>

2. <https://www.securitymagazine.com/articles/98486-435-million-the-average-cost-of-a-data-breach>

3. <https://www.statista.com/statistics/870924/worldwide-digital-transformation-market-size>

Résumé

Aujourd'hui, les entreprises se numérisent à une vitesse fulgurante, dépensant des milliards pour transformer leurs workflows internes et leurs stratégies commerciales. Il est plus que jamais vital de protéger cet investissement.

La moindre violation de données ou interruption de service imprévue risque de nuire à la réputation de l'entreprise, à son infrastructure numérique et à son modèle économique. Pour cette raison, il n'a jamais été aussi important pour les entreprises de se protéger contre la cybercriminalité et d'autres menaces plus physiques ou naturelles qui pèsent sur leur infrastructure numérique.

Pourtant, il n'a jamais été aussi difficile d'atteindre cet objectif. Le volume et la complexité des menaces augmentent et se multiplient en permanence. Qu'il s'agisse de l'augmentation du nombre de ransomware ou de la sophistication croissante des attaques via l'ingénierie sociale, la sécurité n'a jamais été aussi complexe.

La meilleure façon de relever ce défi et d'offrir une protection de pointe est d'adopter une approche de défense approfondie, fondée sur une stratégie de sécurité sophistiquée et multicouche.

Les couches d'une stratégie de sécurité moderne sont les suivantes :

- **Prévention** : cette couche associe des technologies telles que la protection des noeuds d'extrémité et des DNS à une solide formation de sensibilisation à la sécurité afin d'arrêter les menaces avant même qu'elles n'atteignent votre réseau.
- **Protection** : grâce à la protection, au chiffrement et à la continuité des messages électroniques, vous pouvez atténuer le risque de menaces qui endommagent les appareils et les systèmes ou entraînent des temps hors service.
- **Récupération** : avec une sauvegarde et un basculement sophistiqués, ainsi que des mesures SaaS et de continuité des activités, vous renforcez votre solidité et réduisez le délai de récupération.

Ces couches vont de pair avec la formation pour maintenir une culture de sensibilisation à la sécurité parmi tous les collaborateurs. Ces derniers travaillent de manière optimale lorsqu'ils sont soutenus par une couche unique et unifiée de contrôle et d'intelligence de gestion qui donne accès à toutes les données et outils de cybersécurité dont ils ont besoin via une plate-forme consolidée.

OpenText Cybersecurity est un leader du marché de la cybersécurité intelligente pour les entreprises. Grâce à Secure Cloud, cette suite offre aux entreprises un panneau de configuration d'outils de cybersécurité avancés, notamment le chiffrement et la protection des messages électroniques, la sécurité des noeuds d'extrémité, la sauvegarde SaaS (Software-as-a-Service) et l'archivage des informations.

La sécurité multicouche en bref

Prévention

Sécurisation de vos périphériques, de vos utilisateurs et de vos services de noms de domaine



OpenText™ Core Endpoint Protection



OpenText™ Core DNS Protection



OpenText™ Core Security Awareness Training

Protection

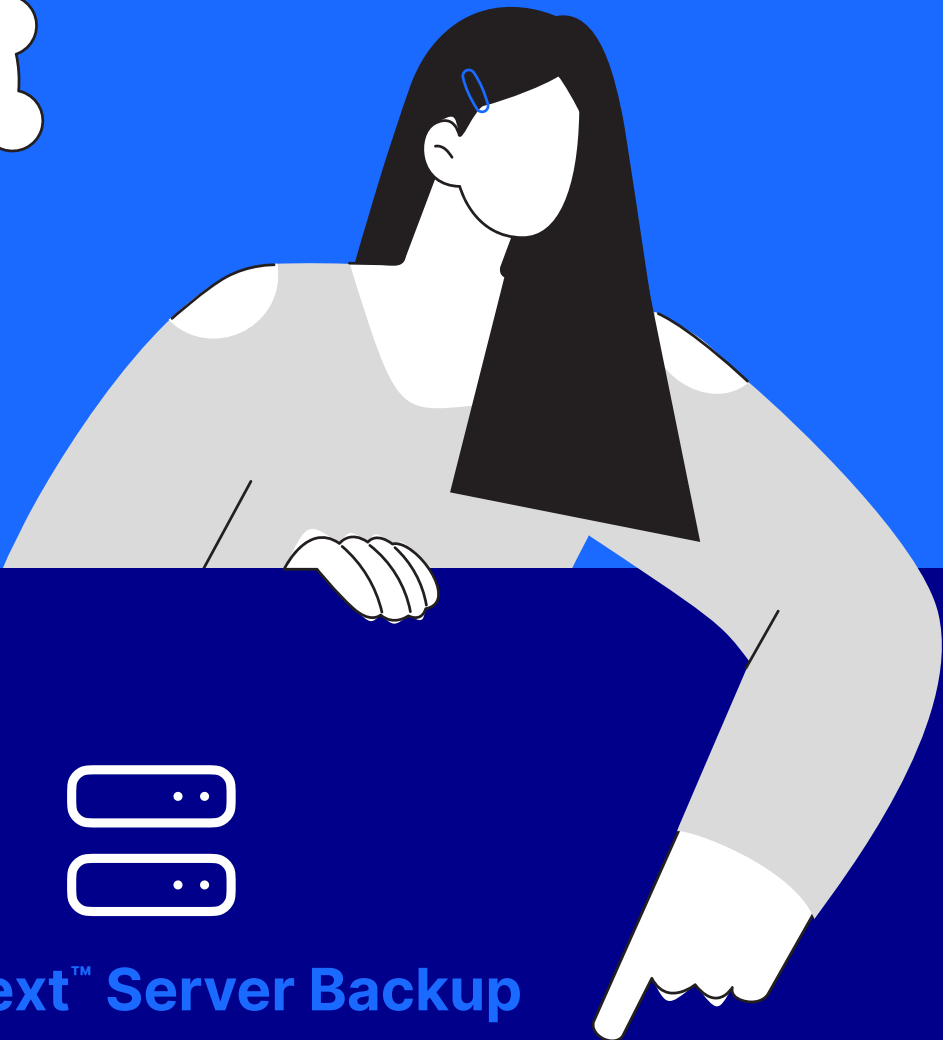
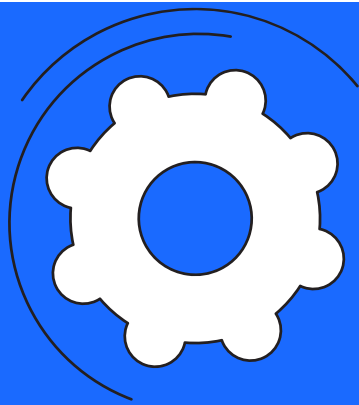
Sécurisation de vos communications et de toutes les données de l'entreprise



OpenText™ Core Email Encryption

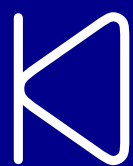


OpenText™ Core Email Threat Protection and OpenText™ Core Email Continuity



Récupération

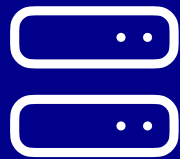
Protection de vos données et continuité des opérations



OpenText™ Recover



OpenText™ Core Cloud-to-Cloud Backup



OpenText™ Server Backup

Pourquoi les entreprises doivent-elles penser cyberrésilience ?

Comme nous l'avons déjà vu, entre un tiers et deux tiers des entreprises (selon leur taille) subissent des attaques de logiciels malveillants au cours d'une année donnée¹. En 2022, selon le FBI, les entreprises américaines ont perdu un total de 10,3 milliards de dollars en raison de violations de données et d'autres types de cybercriminalité⁴.

En 2022, l'incidence de la plupart des types de cybercriminalité est restée élevée :

- Le nombre d'attaques par ransomware a augmenté de 18 %⁵.
- 5,5 milliards d'attaques de logiciels malveillants ont été perpétrées, soit une hausse de 2 % par rapport à l'année précédente⁶.
- Le nombre de tentatives de phishing dans le monde entier a doublé, atteignant 500 millions⁷.
- Le volume des attaques de la chaîne d'approvisionnement a augmenté de plus de 700 %⁸.

Cela se produit à une époque où les entreprises numérisent leurs processus de travail et leurs stratégies de commercialisation à une vitesse fulgurante. 60 % des cadres dirigeants déclarent qu'ils prévoient d'augmenter les dépenses de leur entreprise en matière de transformation numérique⁹.

Cet investissement est précieux et nécessite une protection. Néanmoins, plus une entreprise est numérisée, plus elle est exposée aux menaces qui pèsent sur cet investissement. La solution consiste à passer de la protection de la périphérie du réseau à un modèle de protection multicouche.

4. <https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics>

5. <https://www.statista.com/statistics/1315826/ransomware-attacks-worldwide>

6. <https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide>

7. https://www.kaspersky.com/about/press-releases/2023_the-number-of-phishing-attacks-doubled-to-reach-over-500-million-in-2022

8. <https://www.infosecurity-magazine.com/news/software-supply-chain-attacks-hit>

9. <https://digitalworksgroup.com/investment-in-digital-transformation-will-increase-in-2023>

Le moyen le plus rapide d'obtenir l'expertise de sécurité adéquate

La meilleure façon d'y parvenir est de collaborer avec un fournisseur de technologies capable de proposer une approche de sécurité complète et intégrée : protection des informations, des espaces de travail, des périphériques, des réseaux, des processus et des charges de travail.

Le partenaire doit disposer d'une plate-forme de gestion qui prend en charge une approche de sécurité en couches, afin de rationaliser et d'automatiser les stratégies, les autorisations et les règles métiers au sein du personnel.

Vos administrateurs de sécurité doivent pouvoir, via une interface unique, gérer les mesures de sécurité à l'échelle de l'organisation, appliquer des renseignements sur les menaces en temps réel et des mises à jour de l'état de la sécurité dans l'ensemble de l'infrastructure informatique, ainsi qu'accéder aux outils dont ils ont besoin pour prévenir les violations de données et protéger les actifs où qu'ils se trouvent : sur le cloud, sur site, sur des emplacements distants ou chez les télétravailleurs.

En cas d'incident de cybersécurité, qu'il s'agisse d'une tentative de violation par un cybercriminel ou simplement d'un incident naturel ou artificiel qui affecte la continuité des activités, votre personnel informatique doit disposer de tous les outils dont il a besoin pour récupérer et atténuer les temps hors service, via la même plate-forme consolidée.

La couche de prévention

Comme le dit l'adage : mieux vaut prévenir que guérir. Avec les bons systèmes et la bonne méthodologie, il est possible de détecter et d'intercepter la plupart des cybermenaces avant qu'elles n'entraînent une violation de données ou une perte de service.

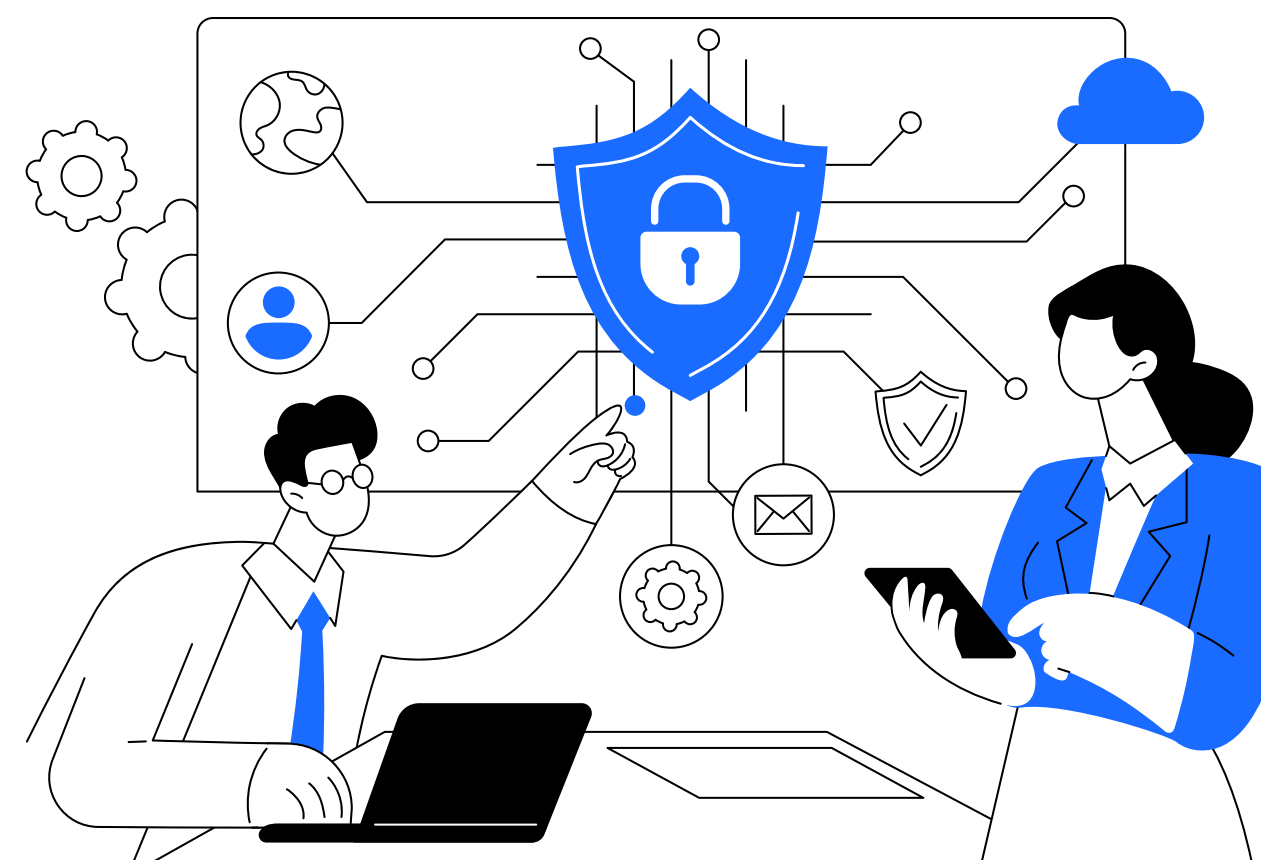
Pour ce faire, vous devez investir dans une couche de prévention leader du marché, ainsi que dans les connaissances et les méthodologies sous-jacentes aux technologies qui composent cette couche.

Voici quelques exemples de technologies de couche de prévention et de mesures de soutien :

- **OpenText Core Endpoint Protection** : protection dynamique des noeuds d'extrémité des fichiers, scripts, URL et exploits malveillants, via une architecture basée sur le cloud.
- **OpenText Core DNS Protection** : la protection DNS intelligente filtre même le trafic DNS chiffré (pour les utilisateurs itinérants et les utilisateurs du réseau), les empêchant ainsi d'accéder à des sites Web inappropriés.
- **Formation de sensibilisation de base à la sécurité OpenText** : empêchez les criminels de manipuler vos employés pour accéder aux réseaux et aux données, grâce à des campagnes de formation fréquentes et automatisées.

Les technologies de prévention doivent être soutenues par une culture de la sécurité. C'est pourquoi il est essentiel de s'assurer que les employés comprennent comment éviter les menaces et comment utiliser au mieux la technologie de la couche de prévention. Cependant, la culture et la technologie de la couche de prévention ne suffisent pas à elles seules. Les deux doivent être soutenues par une couche de coordination intelligente.

Les plates-formes de renseignement sur les menaces, qui exploitent l'intelligence artificielle (IA), devraient fournir aux technologies de la couche de prévention les données dont elles ont besoin pour comprendre à quoi ressemble la « normalité », dans toute une série de contextes différents. Cela leur permet de détecter et d'arrêter instantanément les menaces en cours de développement en temps réel.



La même couche d'assistance sous-jacente devrait permettre au personnel informatique d'accéder instantanément aux technologies de la couche de prévention, mais aussi aux technologies complémentaires d'autres couches, le tout via un seul panneau de configuration. Ainsi, lorsqu'une menace est détectée, votre équipe informatique peut coordonner la réponse dans tous les domaines, rapidement et sans limites.

La couche de protection

La partie suivante de tout système de défense en profondeur est la couche de protection. Si une menace peut pénétrer dans la couche de prévention, les technologies de la couche de protection entrent en action. Elles neutralisent cette menace avant qu'elle ne puisse nuire à vos ressources technologiques ou à votre entreprise.

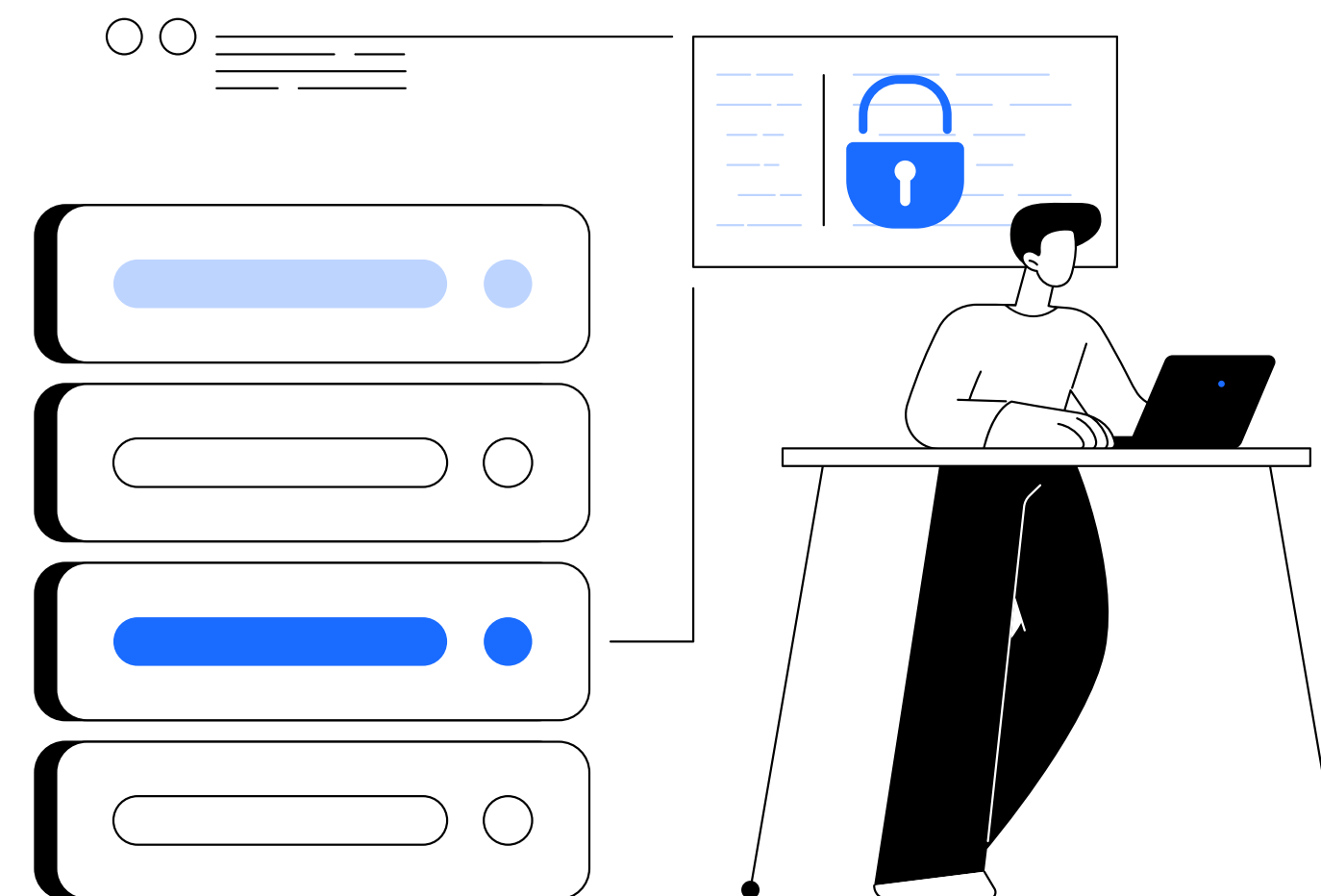
Voici quelques exemples de technologies de couche de protection et de mesures sous-jacentes :

- **OpenText Core Email Threat Protection et OpenText Core Email Continuity** : ces technologies analysent les liens et les pièces jointes des messages à la recherche de logiciels malveillants, et contrôlent même les personnes autorisées à transférer les messages ou à y répondre.
- **Chiffrement des messages électroniques** : protégez les données sensibles et confidentielles grâce à un chiffrement de pointe facile à administrer, invisible pour les utilisateurs et ne nécessitant aucune formation supplémentaire.

En gérant les technologies de la couche de prévention à partir du même écran, votre équipe informatique est en mesure de mettre en place des procédures de sauvegarde dans le cloud afin d'éviter le temps hors service imprévu.

Les mêmes données sur les menaces en temps réel qui sous-tendent les technologies de la couche de prévention, ainsi qu'une méthode de recherche avancée, permettent aux technologies de la couche de protection de détecter les liens malveillants, les pièces jointes et les autres charges utiles. Elles les empêchent ensuite de s'exécuter, ce qui garantit la sécurité de vos systèmes et de vos données.

À l'ère du travail hybride, la couche de protection garantit que chaque nœud, segment de réseau et vecteur d'attaque potentiel est surveillé en permanence et protégé par des technologies de sécurité avancées. Cela vaut pour tous les appareils, logiciels et systèmes, qu'ils soient mobiles ou situés à la périphérie du réseau/dans le réseau.



La couche de récupération

L'ajout d'une couche de récupération à votre architecture de défense en profondeur est essentiel pour atteindre et maintenir la cyberrésilience. En pratique, les couches de prévention et de protection capteront la plupart des menaces entrantes. Il est cependant risqué de s'appuyer uniquement sur les deux premières couches.

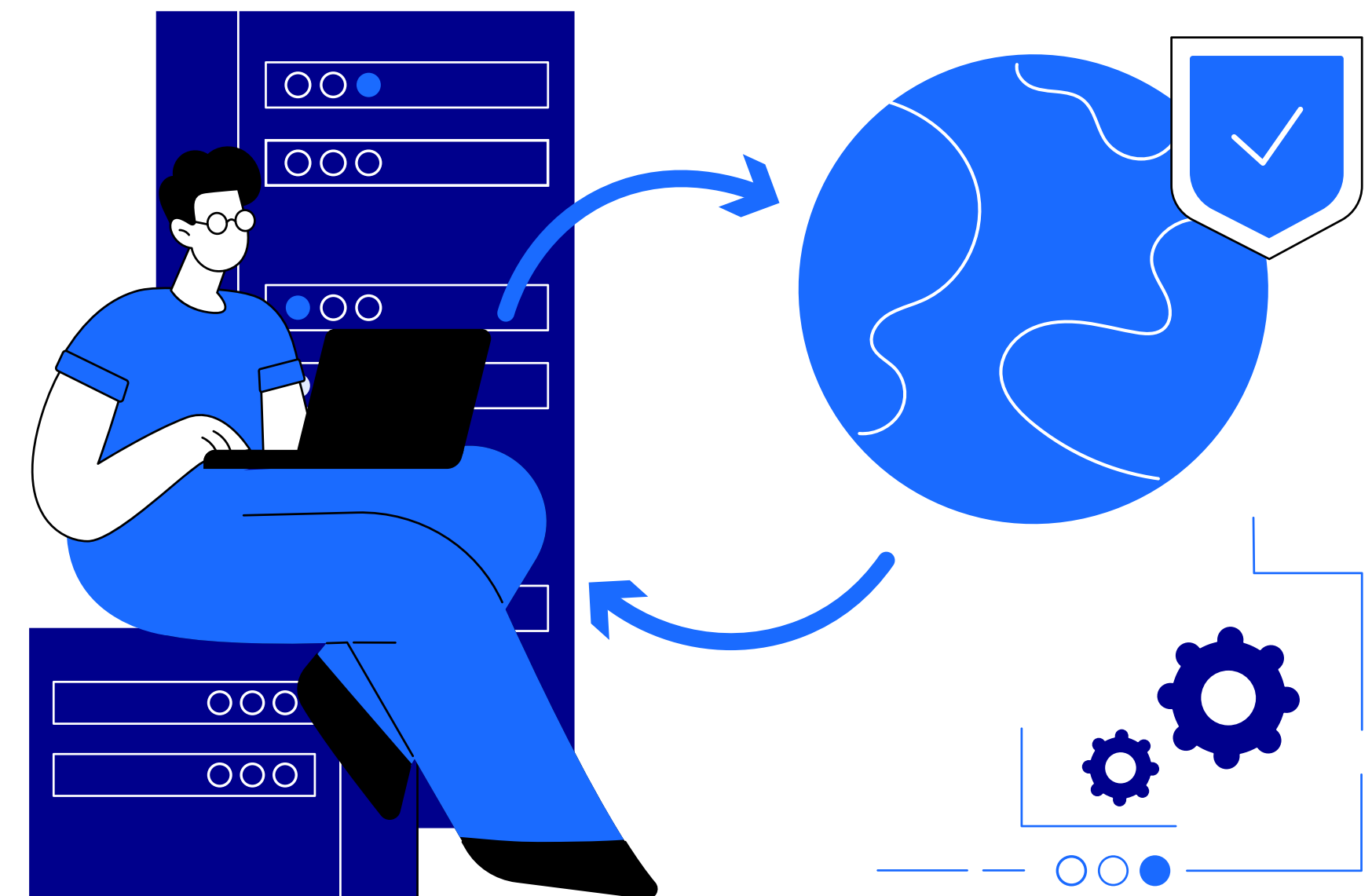
Sans des technologies de reprise robustes, l'entreprise ne peut pas se protéger contre les ransomware, les incendies, les inondations, les coupures de courant et autres catastrophes naturelles ou provoquées par l'Homme. Elle s'expose également à des accusations de non-respect des meilleures pratiques et des exigences réglementaires.

Voici quelques exemples de technologies de la couche de récupération et de mesures prises en charge :

- Continuité des applications SaaS : intégrez la solidité des données aux applications SaaS et aux autres services hors site que vous utilisez, afin de vous protéger contre les pertes dues à des temps hors service imprévus.
- Récupération du système cloud : sauvegardez des serveurs locaux ou cloud, gérez vos sauvegardes et récupérez des données spécifiques ou des systèmes entiers.
- Reprise après sinistre : copies actualisées en permanence de vos serveurs et systèmes critiques, prêtes à basculer en quelques minutes.

Comme pour les autres couches, ces technologies doivent être disponibles via un seul panneau de configuration. L'équipe informatique doit être en mesure de suivre en toute transparence les problèmes en cours de développement à l'aide des différents outils et systèmes disponibles, le tout via une interface unique.

Lorsqu'elle décide qu'il est temps de récupérer des données ou des systèmes, ou de passer entièrement à une sauvegarde de reprise après sinistre, elle doit pouvoir le faire rapidement, avec un overhead réduit au minimum. Cela n'est possible que lorsque tous les systèmes de commande pertinents sont unifiés dans une interface unique et conviviale.



OpenText Cybersecurity : bâtir une activité cyber-résiliente

OpenText Cybersecurity est une nouvelle génération de fournisseurs. Nos outils offrent une approche de la sécurité à plusieurs couches : la prévention, la protection, la récupération et bien plus encore.

Les outils et services de cybersécurité fournis comprennent, sans s'y limiter :



OpenText Core Endpoint Protection : sécurisez vos PC, ordinateurs de bureau et autres noeuds d'extrémité contre les logiciels malveillants et les cyber-attaques les plus sophistiqués.



OpenText Core Security Awareness Training : formation visant à prévenir les comportements risqués des employés pouvant conduire à des compromissions de la sécurité informatique.



OpenText Core Email Threat Protection et OpenText Core Email Continuity : ces technologies détectent dynamiquement les menaces dans les liens et les pièces jointes pour sécuriser les boîtes de réception et les systèmes contre les menaces liées aux messages électroniques.



OpenText Core Cloud-to-Cloud Backup : protégez les données critiques stockées sur des plates-formes cloud et SaaS, grâce à cette sauvegarde automatisée, chiffrée et sécurisée de cloud à cloud.



OpenText Core Email Encryption : chiffrement de qualité industrielle qui s'exécute en arrière-plan, sans perturber les workflows ni nécessiter d'intervention de la part des utilisateurs.



OpenText Core DNS Protection : bloquez les menaces au niveau du domaine, grâce à une protection DNS avancée basée sur des politiques, qui protège même le trafic DNS chiffré.



OpenText Recover : basculez vers une sauvegarde à jour en quelques minutes et en quelques clics, grâce à cette sauvegarde continue et constamment mise à jour des systèmes de serveurs critiques.



OpenText Server Backup : une sauvegarde sécurisée et continuellement mise à jour des serveurs critiques, pour une récupération rapide et un temps hors service quasi nul.

La plupart de ces solutions sont disponibles dans OpenText Secure Cloud : une plate-forme unique qui permet de surveiller et de contrôler tous les services de sécurité, qu'il s'agisse de la prévention, de la protection ou de la récupération. Elle offre à vos équipes informatiques une cyber-intelligence en temps réel et tous les outils dont elles ont besoin pour protéger votre entreprise, votre réputation et votre investissement dans la transformation numérique.

OpenText Cybersecurity offre une protection de pointe aux clients de tous les secteurs d'activité, partout dans le monde. En 2022, OpenText Cybersecurity a aidé ses clients à réduire les taux d'infection par des logiciels malveillants à un cinquième de ce qu'ils étaient en 2020. Nos experts aident les entreprises du monde entier et de nombreux secteurs différents à développer une cyberrésilience de pointe, basée sur une protection multicouche intelligente.

Exemple d'entreprise : compagnie d'assurance santé

Voyons comment une entreprise fictive aux besoins sophistiqués, complexes et exigeants peut bénéficier d'une approche de sécurité multicouche.



Prochaines étapes

La mise en place d'une cyberdéfense en profondeur ne doit pas nécessairement prendre beaucoup de temps ni impliquer des frais généraux initiaux prohibitifs. Avec la bonne approche, la bonne technologie et le bon partenaire, vous pouvez commencer dès aujourd'hui à adopter la sécurité en couches.

OpenText Cybersecurity est un nouveau type de fournisseur pour les entreprises de toutes tailles. Nos experts peuvent vous aider à comprendre la combinaison de technologies dont vous avez besoin pour devenir cyber-résilient et protéger votre investissement dans la transformation numérique. Intégrez la solidité numérique dans votre modèle d'entreprise, avec une approche pérenne, évolutive et adaptable en couches pour la cybersécurité.

Contactez OpenText Cybersecurity dès aujourd'hui pour commencer votre transition vers une cybersécurité plus intelligente et plus simple.

go.zixcorp.com/Email-Security.html

À propos d'OpenText

OpenText Cybersecurity fournit des solutions de sécurité complètes pour les entreprises et les partenaires de toutes tailles. De la prévention à la détection, en passant par la réponse, la récupération, l'enquête et la conformité, notre plate-forme unifiée de bout en bout aide les clients à développer leur cyberrésilience via un portefeuille de sécurité global.

Grâce à des informations exploitables issues de nos renseignements en temps réel et contextuels sur les menaces, les clients d'OpenText Cybersecurity bénéficient de produits hautement efficaces, d'une expérience conforme et d'une sécurité simplifiée pour les aider à gérer les risques métiers.

À propos d'OpenText

OpenText, The Information Company, permet aux organisations d'obtenir des informations grâce à des solutions de gestion des informations leaders sur le marché, sur site ou dans le cloud. Pour plus d'informations sur OpenText (NASDAQ : OTEX, TSX : OTEX), consultez le site opentext.com

opentext.com | [X \(anciennement Twitter\)](#) | [LinkedIn](#) | [Blog du PDG](#)