

Gewährleistung des Vertrauens in Daten für eine sichere KI-Einführung

Erstellen und pflegen Sie vertrauenswürdige Daten für den effektiven Einsatz von KI in Ihrem Unternehmen



Vorteile

- Geringeres Datenrisiko bei der Einführung von KI.
- Schutz Ihrer KI-Datenpipelines.

Künstliche Intelligenz (KI) bietet enorme Chancen und verändert die heutige Unternehmenslandschaft. Es gibt viele KI-Tools auf dem Markt, die überzeugende Geschäftsergebnisse und Effizienzsteigerungen ermöglichen. Angesichts der tiefgreifenden Auswirkungen von KI-Investitionen ist die Einführung dieser Technologie für Unternehmen zu einer strategischen Notwendigkeit geworden, um ihre Wettbewerbsfähigkeit zu erhalten.

IDC Global DataSphere prognostiziert, dass die Datenmenge in den nächsten fünf Jahren mit einer durchschnittlichen jährlichen Wachstumsrate von 21,2 % steigen und bis 2026 mehr als 221.000 Exabyte (ein Exabyte entspricht 1.000 Petabyte) erreichen wird.¹ Diese Datenexplosion stellt bereits vor der Einführung von KI eine große Herausforderung dar. Die Bewältigung der Datenflut – ihre Auswirkungen auf die Datenqualität, die Produktivität der Endbenutzer und die Betriebskosten – ist für die effektive Verwaltung wachsender Datenbestände und die Minderung von Sicherheitsrisiken von entscheidender Bedeutung.

Vertrauenswürdige Daten während des gesamten Datenlebenszyklus bilden die Grundlage für eine erfolgreiche KI-Implementierung und beeinflussen direkt die Genauigkeit, Zuverlässigkeit und Integrität der KI-Systeme Ihres Unternehmens. Die OpenText Datensicherheitsplattform bietet Ihnen umfassende Tools, mit denen Sie hochwertige Daten für KI-Systeme verantwortungsbewusst kuratieren können.

¹ IDC, [High Data Growth and Modern Applications Drive New Storage Requirements in Digitally Transformed Enterprises, 2022](#)

Unsere führende Datensicherheitsplattform bietet zuverlässige KI durch:

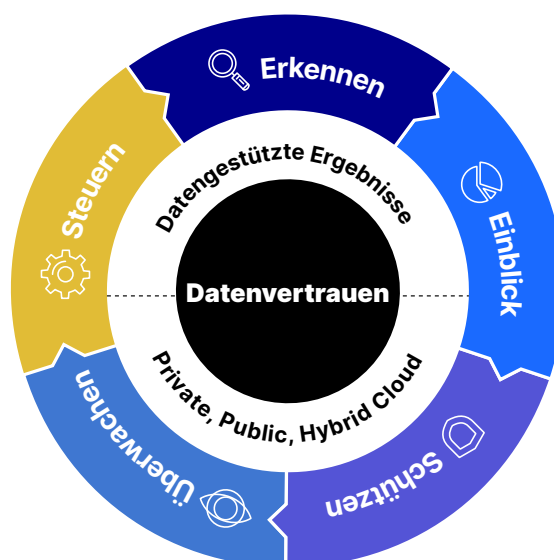
- **Verbesserte Datensicherheit:** Die Implementierung strenger Datensicherheitsmaßnahmen reduziert Risiken wie Datenverletzungen und -vergiftungen und gewährleistet die Integrität und Zuverlässigkeit von Daten für KI-Systeme.
- **Verbesserte Daten-Governance:** Eine effektive Verwaltung des Datenlebenszyklus hilft dabei, die Datenflut zu bewältigen, die Speicherung zu optimieren und die Einhaltung von Vorschriften zu gewährleisten, wodurch das allgemeine Datenrisiko reduziert wird.
- **Genauere Datenanalyse:** Fortschrittliche Analysen und kontextsensitive Grammatiken identifizieren und klassifizieren sensible Daten genau und verbessern so den Datenschutz und die betriebliche Effizienz.
- **Umfassender Datenschutz:** Gewährleisten Sie durchgängige, datenzentrierte Sicherheit über den gesamten Datenlebenszyklus hinweg. Und beheben Sie Risiken durch den Einsatz führender Schutztechniken – einschließlich Anonymisierung –, um Ihre Daten vor Angreifern zu schützen, ohne Anwendungen, Datenbanken oder die Leistung zu beeinträchtigen.
- **Proaktive Datenüberwachung:** Die kontinuierliche Überwachung des Datenzugriffs und der Datennutzung stellt sicher, dass nur autorisierte Benutzer auf sensible Daten zugreifen können, und unterstützt damit IT-Modernisierungs- und Nachhaltigkeitsinitiativen.

Geringeres Datenrisiko bei der Einführung von KI

Um Vertrauen in Ihre KI-Daten zu schaffen, ist es unerlässlich, robuste Datensicherheitspraktiken zu implementieren und qualitativ hochwertige Daten zu kuratieren – denn hervorragende KI basiert auf außergewöhnlichen Daten. Als wichtige Grundlage, die KI-Anwendungsfälle und andere Anforderungen in den Bereichen Datensicherheit, Datenschutz und Governance ermöglicht, bietet unsere Datensicherheitsplattform durch ihre Cloud-Architektur erhebliche Vorteile. Die Plattform bietet eine einheitliche Einrichtung, Erkennung, Klassifizierung, Verwaltung, zentralisierte Analyse und hohe Skalierbarkeit.

Bei OpenText sind Sicherheit, Datenschutz und Governance von Daten miteinander verknüpft. Unsere Technologien zur Verbesserung des Datenschutzes bilden eine verbindende Brücke zwischen diesen Anwendungsfällen, um Ihre sensiblen Daten zu erkennen, zu analysieren und zu schützen. Unsere innovativen Funktionen ermöglichen es Unternehmen, die Datennutzung kontinuierlich zu überwachen – wer hat Zugriff auf welche Daten – und Daten während ihres gesamten Lebenszyklus zu verwalten.

Durch den Einsatz modernster Technologien wie KI-gesteuerte PII-Erkennung, Verschlüsselung, Maskierung/Anonymisierung, Tokenisierung und Datenminimierung können Sie Daten sorgfältig kuratieren, um sie sicher und ethisch in LLMs und GenAI-Plattformen zu verwenden. Mit diesem Ansatz können Sie sicher Trainingsmodelle erstellen und die Vorteile der KI voll ausschöpfen. Unsere Plattform unterstützt Sie dabei, sicherzustellen, dass personenbezogene Daten während der Nutzung – auch im Zusammenhang mit Datenanalysen – sicher sind und ethisch behandelt werden, um sie vor möglichen Schäden zu schützen.



Schutz Ihrer KI-Datenpipelines

Unsere einheitliche Datensicherheitsplattform unterstützt Sie beim Aufbau einer umfassenden Grundlage für Ihr AI-bezogenes Datensicherheitsmanagement mit branchenführenden Funktionen in allen Bereichen der Datensicherheit:

- Datenanalysen
- Datenklassifizierung
- Datenschutz
- Datenüberwachung
- Governance von Datenlebenszyklen

Datenanalysen

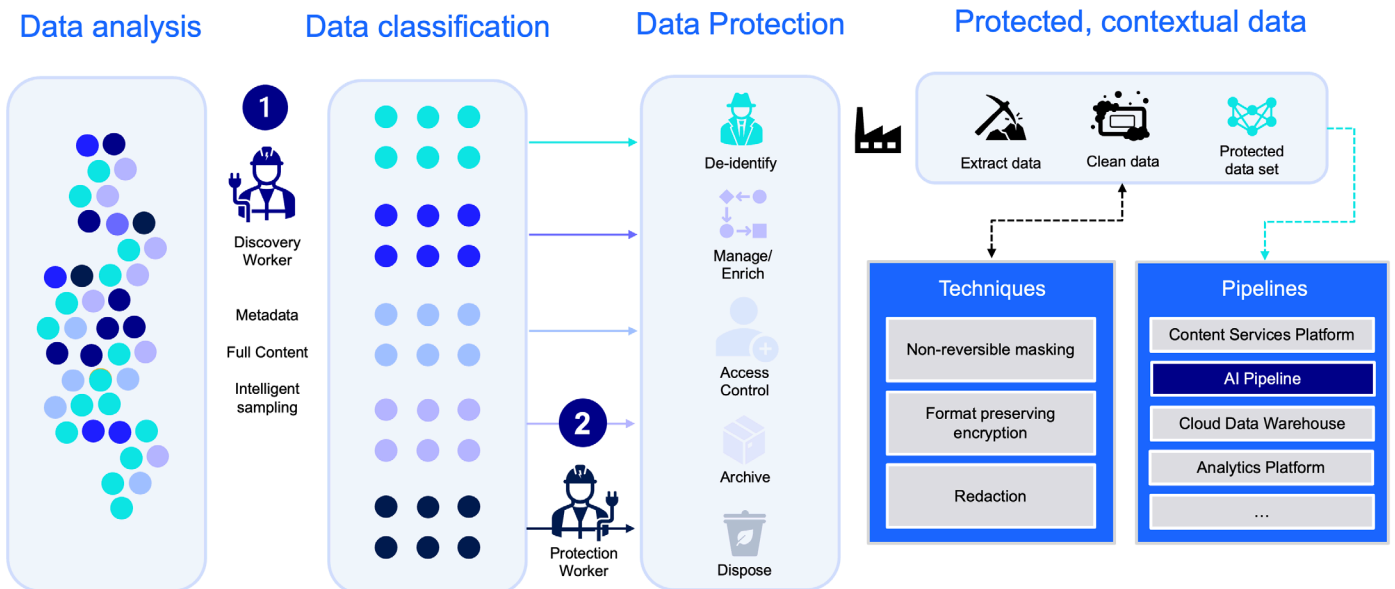
Sichern Sie Ihre Datenpipelines mit der Datensicherheitsplattform von OpenText

Um Ihre KI-Datenpipeline zu schützen, ist es entscheidend, zunächst den Speicherort sensibler Daten zu ermitteln. Unsere Plattform bietet umfassende Datenerkennung durch Scannen, Tagging, Analysen, Risikomessung und Erkennung personenbezogener Daten in strukturierten und unstrukturierten Repositories. Diese Transparenz gewährleistet, dass Sie Ihre sensiblen Daten effektiv schützen können.

Die cloudgestützte Datenerkennung der Plattform umfasst Dateisysteme, Datenbanken und Cloud Data Warehouses. Dank schneller und intelligenter Scanfunktionen identifiziert OpenText risikobehaftete Datenrepositories innerhalb von Tagen statt Wochen und optimiert so Ihren Erkennungsprozess.

OCR-Funktionen verbessern die Erkennung sensibler Daten in gescannten Bildern und Mediendateien und gewährleisten eine gründliche Identifizierung von Unternehmensinformationen. Über sensible Daten hinaus identifiziert die Plattform redundante, veraltete und triviale Daten, optimiert die Speicherung und reduziert Sicherheitsrisiken.

Erkennung und Anonymisierung sind wesentliche Elemente jeder Datensicherheits- und KI-Strategie.



Datenklassifizierung

Die Bestimmung der Bedeutung und des Werts Ihrer Daten ist entscheidend für die Risikominimierung und die Operationalisierung von Datenschutz und Datenanalysen für die Einführung von KI. Die Datensicherheitsplattform von OpenText nutzt leistungsstarke Analysen, um sensible Datenelemente zu identifizieren, die geschützt werden müssen.

Unsere Kerngrammatik legt den Schwerpunkt auf folgende Daten:

Datenklassifizierung	Beschreibung
PII	Persönlich identifizierbare Informationen, darunter 13 Entitätskategorien in mehr als 38 verschiedenen Ländern
PHI	Geschützte Gesundheitsdaten, die in der Regel mit der nordamerikanischen Gesundheitsbranche in Verbindung stehen
PCI	Daten der Zahlungskartenbranche, z. B. Kreditkarten und primäre Kontonummern
IP	Geistiges Eigentum, anpassbar an Ihr Unternehmen.

Der Kontext ist entscheidend und Genauigkeit ist unerlässlich. Unsere Cloud-Plattform basiert auf OpenText IDOL Analytics und bietet kuratierte und optimierte Grammatiken, die entwickelt wurden, um die heutigen globalen Herausforderungen im Bereich des Datenschutzes zu bewältigen. Sie unterstützt die Entitätsextraktion für mehr als 38 Landersprachen, Datenformate und Wirtschaftsregionen:

- Unsere Grammatiken verwenden außerdem Kontext und „Landmarken“, um eine Risikobewertung zu generieren, mit der wir genauere Ergebnisse liefern und Fehlalarme herausfiltern können.
- Die Genauigkeit und der Risikowert basieren auf der Nähe zur identifizierten, extrahierten oder abgeglichenen Entität in Kombination mit ausgefeilten probabilistischen Modellen und Algorithmen zur Verarbeitung natürlicher Sprache, die zur Bestimmung der Stärke der Beziehung und zur Erhöhung des Wertes verwendet werden.
- Die erweiterte Sprachunterstützung in Grammatiken hilft auch beim Kontext, um die Sensibilität oder sogar das Vorhandensein von PII zu bestimmen.
- Es können mehrere Grammatiken kombiniert werden, um Entitäten breiter anzusprechen, was jedoch zu höheren Rechenkosten und längeren Verarbeitungszeiten führen kann.
- Die anpassbare Risikobewertung und Gewichtung von Kategorien bietet Ihnen mehr Flexibilität bei der Auswahl und Konfiguration von Grammatiken, um Ihren Anforderungen gerecht zu werden.

Datenschutz

Mit OpenText können Sie Daten während ihres gesamten Lebenszyklus schützen – vom Zeitpunkt ihrer Erfassung bis hin zu ihrer Weitergabe innerhalb Ihres gesamten Unternehmens –, ohne dass Live-Informationen erhöhten Risiken oder Bedrohungen ausgesetzt werden. Das ist der Kern des datenzentrierten Schutzes.

Mit unseren Datenschutztechnologien erhalten Sie die Kontrolle über Ihre sensiblen Daten, unabhängig davon, ob diese gespeichert, übertragen oder verwendet werden. Unabhängig davon, ob Sie einen oder Hunderte von Anwendungsfällen implementieren, lässt sich unsere Technologie skalieren, um alle Datenschutzerfordernungen vor Ort und in einer Multi-Cloud-Hybrid-IT zu erfüllen. Unsere Lösung anonymisiert Daten, sodass sie für Angreifer unbrauchbar werden, während ihre Verwendbarkeit, Nützlichkeit und referenzielle Integrität für Datenprozesse, Anwendungen und Dienste erhalten bleibt. Mit OpenText können Sie die Gefahr von Datenverletzungen neutralisieren, indem Sie Ihre geschützten Daten für Angreifer wertlos machen, unabhängig davon, ob sie sich in Produktions-, Analyse-, Test- und Entwicklungssystemen befinden oder extern geteilt werden.

Ressourcen

Bewältigung der Schnittstelle zwischen KI und finanziellem Risiko: Ein proaktiver Ansatz

[Blog-Beitrag lesen](#) ›

Drei Schritte zur Entschlüsselung des Datenrisikos

[Sehen Sie sich die Infografik an](#) ›

Leitfaden von OpenText zu Datensicherheit und der Verringerung des finanziellen Risikos

[Video ansehen](#) ›

Unser einzigartiger, bewährter datenzentrierter Schutzansatz, bei dem die Zugriffsrichtlinie mit den Daten selbst übertragen wird, ermöglicht Datenschutz ohne Änderungen am Datenformat oder der Datenintegrität und eliminiert die Kosten und die Komplexität der Ausstellung und Verwaltung von Zertifikaten und Schlüsseln. Infolgedessen haben unsere [Kunden aus verschiedenen Branchen](#) in nur 60 bis 90 Tagen einen durchgängigen Datenschutz im gesamten Unternehmen erreicht. Dieser Erfolg ist auf die minimalen, in den meisten Fällen gar keinen Auswirkungen auf Anwendungen und Datenbankschemata zurückzuführen.

Datenüberwachung

Mit unseren Funktionen für die Datenzugriffssteuerung kann Ihr Unternehmen sicherstellen, dass nur autorisierte Benutzer mit bestimmten Rollen auf Ihre KI-Datenpipelines und andere privilegierte Daten zugreifen können. Sie profitieren von umfassenden Funktionen, darunter Änderungsbenachrichtigungen, Lebenszyklusmanagement, Sicherheitssperren und Sicherheitsbarrieren. Dank der detaillierten Berichtsfunktionen lassen sich Daten, die verschoben, gesichert oder gelöscht werden müssen, leicht identifizieren.

OpenText Database Activity Monitoring überwacht Datenbanken aktiv in Echtzeit und generiert umgehend Warnmeldungen bei Verstößen gegen Richtlinien. Dabei werden eine Vielzahl von Aktivitäten abgedeckt, darunter Datenmanipulation, Schemaänderungen, Änderungen der Zugriffskontrolle und Transaktionskontrolle. Sie können diese Informationen nutzen, um Datenbanken zu identifizieren, die stillgelegt werden sollten, und Einblicke in Anwendungen zu gewinnen, die mit sensiblen Daten interagieren. So können Sie Ausfälle verhindern oder minimieren, den Datenschutz verbessern, IT-Modernisierungsbemühungen unterstützen und Green-IT- und Nachhaltigkeitsinitiativen fördern.

Daten-Governance

Die zunehmende Verbreitung von Daten und Anwendungen hat kontinuierlich zu einer Anhäufung redundanter Daten geführt (Duplikate und Kopien von Daten, die über das gesamte Unternehmen und in Cloud-Repositorys verteilt sind). Das Gleiche gilt für veraltete, nicht mehr aktuelle Daten (Daten, auf die über einen längeren Zeitraum nicht zugegriffen wurde) oder Daten von geringem Wert, die lediglich Speicherplatz und Ressourcen für die Verwaltung beanspruchen (Daten wie Urlaubsfotos oder DLL- oder EXE-Dateien).

Eine gut strukturierte Datenmanagementstrategie für Ihre KI-Governance und allgemeine Geschäftspraktiken umfasst Maßnahmen zum Datenlebenszyklus – wie Datenlöschung, Datensatzdeklaration und Archivierung –, die für die Einhaltung verschiedener Vorschriften, die Minimierung von Datenrisiken und die Senkung der Datenspeicherkosten unerlässlich sind. Durch die sorgfältige Umsetzung vertretbarer Datenlöschungsverfahren können Sie Korrekturmaßnahmen anwenden, um den Zugriff zu kontrollieren und hochwertige Daten sicher zu verwalten.

Die nächsten Schritte:

KI ist nicht länger abstrakt. Sie ist bereits Realität, und die Mitarbeiter in Ihrem Unternehmen nutzen wahrscheinlich bereits KI-Tools wie LLMs. Um diese Tools jedoch optimal und sicher in Ihrem gesamten Unternehmen einzusetzen, ist ein ernsthaftes Engagement für Datensicherheit erforderlich – einschließlich Analyse, Klassifizierung, Schutz, Überwachung und Governance. Wir sind bereit, Ihnen dabei zu helfen, sich mit Tools, die Ihnen bei all diesen Aufgaben unterstützen, einen Wettbewerbsvorteil zu verschaffen.

Sind Sie bereit, mehr über unsere Produkte zu erfahren?

<https://www.opentext.com/products/data-discovery-protection-and-compliance>