Der CISO-Guide: So machen Sie Ihre Datensicherheit mit KI-basiertem DSPM zukunftsfähig

2025

Inhaltsverzeichnis

Orientierung in der unübersichtlichen Datensicherheitslandschaft

Exponentiell wachsende und über zahlreiche Plattformen verteilte Daten erhöhen für viele Unternehmen die Komplexität und damit auch Kosten und Risiken. Für Sicherheitsverantwortliche ist es heute eine echte Herausforderung, volle Transparenz über ihre kritischen Daten zu gewinnen und diese effizient zu kontrollieren. Noch komplexer wird die Lage durch die schnelle Einführung von KI. Sie verstreut Daten zusätzlich und macht Unternehmen anfälliger für Compliance- und Datensicherheitsrisiken.

Wer Risiken minimieren und die Compliance stärken will, braucht Tools, die lückenlose Echtzeit-Transparenz über das komplette Datenuniversum bereitstellen. Genau das liefert Data Security Posture Management (DSPM) — ein moderner Ansatz, der Sicherheitsverantwortliche mit KI und Automatisierung kontinuierlich über alle Daten und Risiken informiert.

Dieses E-Book beleuchtet das enorme Potenzial von DSPM und gibt Sicherheitsverantwortlichen die Werkzeuge an die Hand, um sensible Daten proaktiv zu schützen. Es richtet sich gezielt an erfahrene Sicherheits- und Riskoverantwortliche und bietet konkrete Handlungsempfehlungen für den Umgang mit den Herausforderungen der heutigen Datensicherheitslandschaft. Dieser umfassende Leitfaden zeigt die wichtigsten Trends, Herausforderungen und modernen Strategien im Bereich der Datensicherheit — und unterstreicht, warum DSPM im Zeitalter der KI eine zentrale Rolle beim Schutz Ihrer Daten spielt.

Die zentrale Aufgabe für CISOs: Datensicherheit im KI-Zeitalter souverän gestalten

Für Chief Information Security Officers (CISOs) wird die schnelle Einführung von KI- und Cloud-Technologien zur echten Zwickmühle. So groß die Chancen für Kosteneinsparungen, bessere Geschäftsergebnisse und mehr Produktivität auch sind — die digitale Transformation schafft gleichzeitig zahlreiche neue Datensicherheitsrisiken.

Die rasant wachsende Datenlandschaft

Der Kern des Problems sind die rasant wachsenden Datenmengen in Unternehmen. Sensible und geschäftskritische Daten sind heute nicht mehr an einem zentralen Ort gespeichert, sondern überall verteilt — in KI-Ökosystemen, SaaS- und PaaS-Umgebungen, Multicloud-Bereitstellungen, hybriden Cloud-Architekturen und sogar in herkömmlichen On-Premise-Systemen. Die Zahlen sind überwältigend: IDC prognostiziert ein jährliches Datenwachstum von 21,2 %, das bis 2026 mehr als 221.000 Exabyte erreichen soll.

Umgang mit Komplexität und Risiko

Die Herausforderung für CISOs ist gewaltig: Daten werden ständig erstellt, geteilt und in hunderten verschiedenen Systemen und Anwendungen gespeichert, während die Datenlandschaft immer größer und flüchtiger wird.

Den vollständigen Schutz dieser Informationen zu gewährleisten, ist eine Mammutaufgabe.

Zentrale Datensicherheitsrisiken im Zeitalter der KI:

- **Schwachstellen und Compliance-Risiken:** Fragmentierte und verstreute Daten erhöhen das Risiko für Datenverluste und Compliance-Verstöße. Die Einhaltung von Datenschutz- und Governance-Regeln (DSGVO, CCPA usw.) wird dadurch zu einer großen Herausforderung.
- **Gefahr von ROT-Daten:** Unkontrollierte Schattendaten (unbekannte oder unautorisierte Datenkopien) und verwaisten Daten (veraltete oder vergessene Daten) schaffen kritische Sicherheitslücken. Sie führen häufig zu erheblichen Schwachstellen und vergrößen die Angriffsfläche exponentiell.
- **Generative KI (GenAI) & LLM-Sicherheitsrisiken:** Mit der zunehmenden Nutzung von generativer KI und Large Language Models (LLMs) entstehen neue, spezifische Risiken. Dazu zählen Schatten-KI, Datenlecks (unbeabsichtigte Offenlegung sensibler Informationen), Berechtigungsprobleme innerhalb von KI-Systemen und neue regulatorische Fallstricke. Sorgfältige KI-Sicherheit und LLM-Daten-Governance sind daher unverzichtbar.

Um diese komplexen Herausforderungen zu meistern, brauchen CISOs einen strategischen und proaktiven Ansatz: Starke Daten-Governance, moderne Datenschutzlösungen und durchdachte KI-Sicherheits-Frameworks sorgen dafür, dass sensible Informationen auch in dynamischen Umgebungen geschützt bleiben.

Risiko des Verlusts wertvoller Daten

Angesichts der ständig zunehmenden Zahl gezielter Angriffe und eines dynamischen regulatorischen Umfelds ist es für CISOs entscheidend geworden, die Sicherheit dieser Umgebungen in den Vordergrund zu stellen. Etwa 44 % der Unternehmen haben in den letzten 12 Monaten eine Datenpanne in ihrer Cloud-Umgebung erlebt.[1] Eine solche Sicherheitsverletzung kann schwerwiegende Folgen haben — von Datenverlust über Reputationsschäden bis hin zu finanziellen Einbußen. Mit der wachsenden Bedrohung durch KI- und Cloud-Angriffe gewinnt die Rolle des CISO immer mehr an Bedeutung.

4,44 Mio. USD

Die durchschnittlichen Kosten einer Datenpanne im Jahr 2025[2]

1. Infosecurity Magazine, **Cloud Breaches Impact Nearly Half of Organizations**, 25. Juni 2024.
2. **IBM's Cost of a Data Breach Report 2025**

Um diese Risiken zu bewältigen und die Einhaltung der Vorschriften zu gewährleisten, müssen Sicherheitsverantwortliche ihre Datenumgebungen genau verstehen. Aufgrund des Volumens, der Vielfalt und der Dynamik der Daten stellt deren Sicherung jedoch oft eine Herausforderung dar. Sicherheitsverantwortlichen fehlen häufig Antworten auf diese Fragen:

- Wo sind die Daten?
- Welche Datenspeicher enthalten wertvolle oder vertrauliche Daten?
- Welche Personen, Anwendungen oder KI-Tools greifen auf diese Datenspeicher zu?
- Wie haben KI-Tools Zugriff auf die Daten oder wie werden sie geteilt?
- Wie wertvoll sind die Daten?
- Wie werden die Daten verarbeitet und welche Auswirkungen hat dies auf die Compliance?

Die Grenzen der klassischen Datensicherheit im Zeitalter der KI

Die Spielregeln der Datensicherheit haben sich komplett gewandelt. Lange Zeit haben CISOs versucht, die wachsende Bedrohungslage mit immer mehr Einzellösungen in den Griff zu bekommen. Doch dieser Flickenteppich aus Tools liefert nicht mehr das, was heute wirklich zählt: Klarheit, Kontrolle und wirksamen Schutz.

Die ungelösten Herausforderungen der KI-Sicherheit

Klassische Sicherheitslösungen können mit den Besonderheiten moderner KI nicht Schritt halten. Sie erfassen weder die neuartigen Verhaltensweisen, noch die spezifischen Risiken oder Governance-Anforderungen, die LLMs, generative KI-Agenten und andere Foundation Models mit sich bringen. Für diese neuen Bedrohungen braucht es einen neuen Sicherheitsansatz.

Zeit für ein neues Sicherheitskonzept

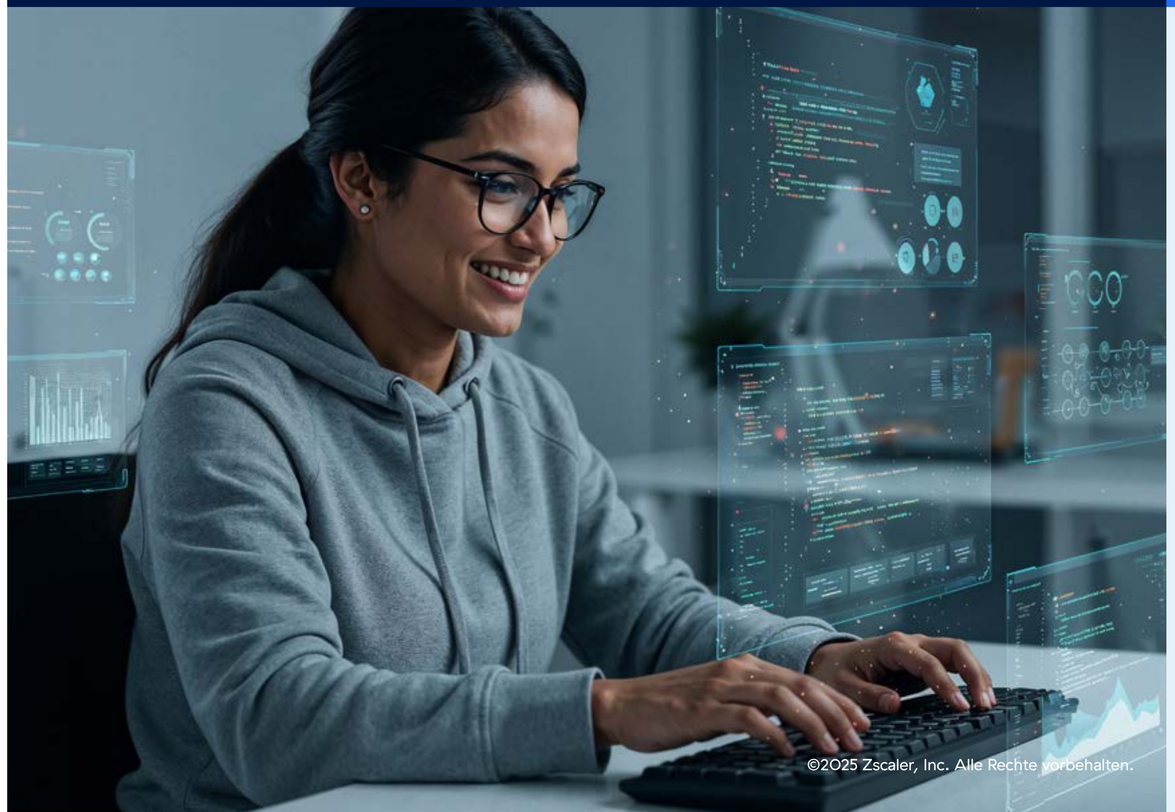
Angesichts der aktuellen Bedrohungen benötigen Sie mehr als nur neue Lösungen. Heute brauchen Unternehmen einen ganzheitlichen, integrierten Ansatz, der Daten-Governance und KI-Sicherheit zusammenbringt. Kurz gesagt: KI-Sicherheit gehört ins Zentrum Ihrer Cybersicherheitsstrategie — nicht an den Rand.

Mehr Sicherheit mit weniger Budget

Knappere Budgets zwingen Sicherheitsverantwortliche dazu, jeden Euro, der ins Sicherheitsportfolio fließt, kritisch zu bewerten. Dadurch ergeben sich klare Prioritäten: Komplexität reduzieren, Kosten senken und gleichzeitig das Sicherheitsniveau deutlich erhöhen. Interessanterweise spielt KI hier eine doppelte Rolle. Trotz aller Risiken gehören ausgereifte, KI-basierte Sicherheitslösungen zu den wirkungsvollsten Investitionen. Sie liefern durchgängige Transparenz, erkennen Bedrohungen schneller und machen Reaktionen auf Vorfälle wesentlich effizienter — ein echter Gewinn für die gesamte Sicherheitsarchitektur.

97 %

der Unternehmen, die einen KI-bezogenen Sicherheitsvorfall meldeten, verfügten nicht über eine angemessene Zugriffskontrolle für KI.[3]



3. IBM's Cost of a Data Breach Report 2025

DSPM als neuer Standard für Datensicherheit im Zeitalter von KI

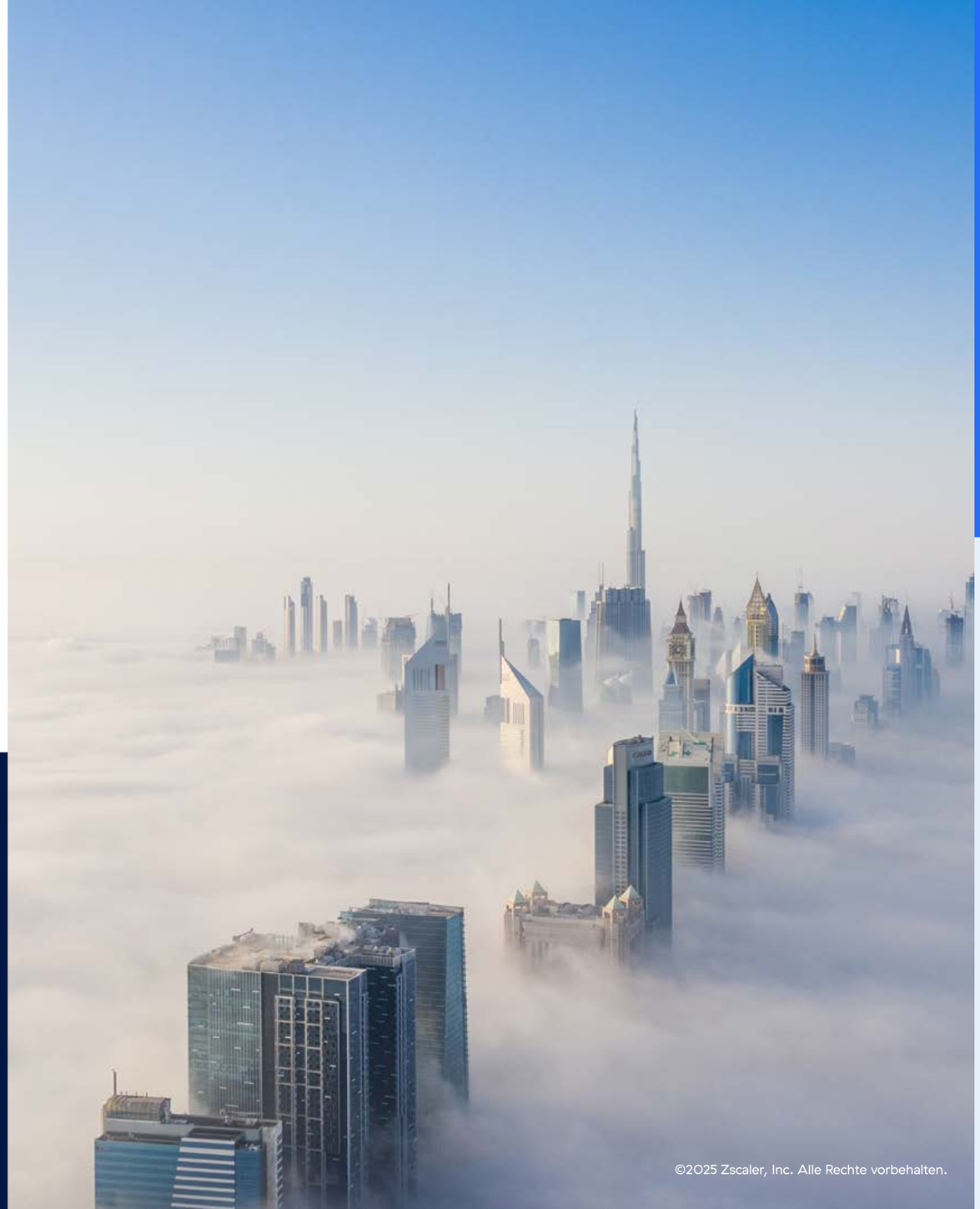
Bei den heutigen KI-Risiken und den offensichtlichen Schwächen herkömmlicher Sicherheitslösungen führt an einem modernen Ansatz für Datensicherheit kein Weg vorbei. Hier erweist sich Data Security Posture Management (DSPM) als zentrale und unverzichtbare Lösung.

DSPM bietet den erforderlichen Kontext und die Automatisierung, um die Komplexität moderner Datenlandschaften gekonnt zu bewältigen. Durch einen vorausschauenden Ansatz sind CISOs in der Lage, ihre Daten besser zu verstehen, Compliance sicherzustellen und die mit KI verbundenen Risiken deutlich zu senken.

4. Ebenda.

1,9 Mio. USD

Durchschnittliche Kosteneinsparungen von Organisationen, die KI-gestützte Sicherheit und Automatisierung nutzen[4]



So stärken CISOs ihre Datensicherheit mit integriertem DSPM

Im Folgenden werden einige Möglichkeiten vorgestellt, wie CISOs KI, ML und Risikokorrelation effektiv nutzen können, um die Datensicherheit zu verbessern:

Risiken durch Schatten-KI, sensible Daten und verwaiste Datensätze in den Griff bekommen

Schattendaten Schattendaten und verwaiste Daten stellen erhebliche Sicherheitsrisiken dar, da sie sich häufig etablierten IT-Sicherheitsrichtlinien und Daten-Governance-Frameworks entziehen. Laut IBM waren 35 % aller Datenpannen auf Schattendaten zurückzuführen und dadurch im Schnitt 16 % teurer. Zudem dauerten es 26,2 % länger, solche Vorfälle zu erkennen, und 20,2 % länger, sie einzudämmen[5]. Schattendaten können in unstrukturierten Dateien, strukturierten Datenbanken, Cloud-Speichern oder auf persönlichen Geräten ohne angemessene Kontrolle vorhanden sein. Verwaiste Daten ohne Lebenszyklusmanagement entwickeln sich ebenfalls schnell zu einem ernsthaften Risiko.
DSPM-Lösungen nutzen KI, um Datenbestände kontinuierlich zu identifizieren und so die Transparenz über die gesamte Datenlandschaft zu erhöhen. KI kann beim Katalogisieren von Dark Data und Schattendaten helfen und so die Transparenz verbessern. Darüber hinaus macht sie Sicherheitsverantwortliche auf potenzielle Risiken aufmerksam und minimiert das Risiko von Sicherheitsverletzungen. Sie kann auf Auffälligkeiten beim Datenzugriff und Muster achten, Anomalien erkennen und potenzielle Sicherheitsverletzungen vorhersagen.

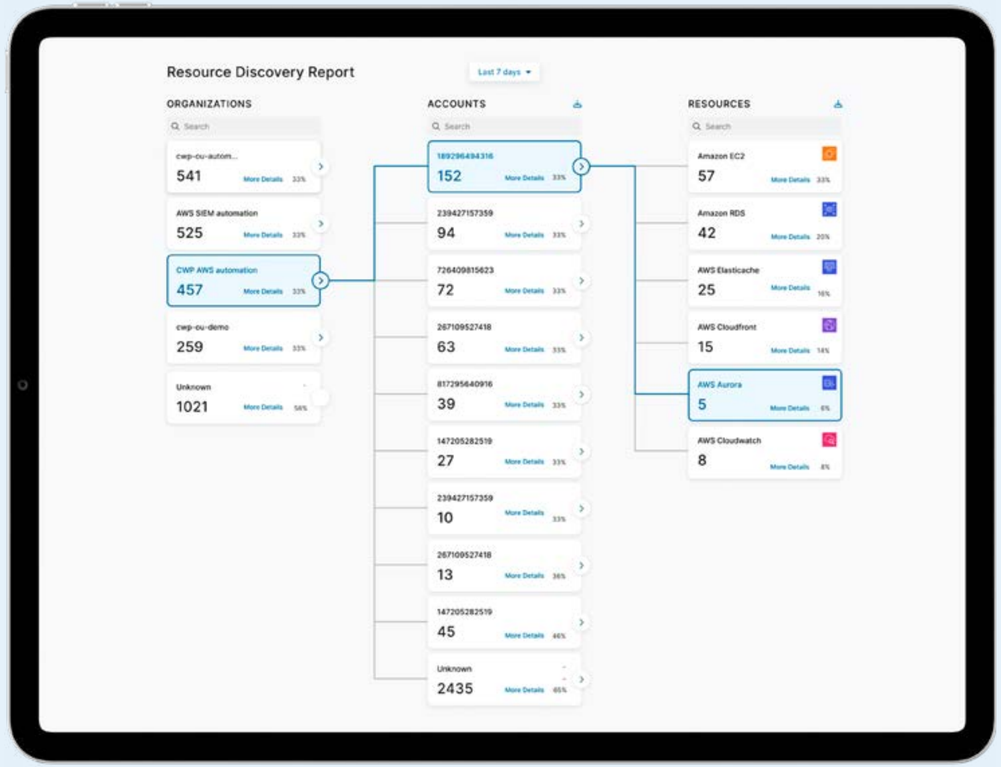
Schatten-KI Ähnlich wie Schatten-IT bezeichnet Schatten-KI vor allem die Nutzung nicht genehmigter KI-Tools, die auf sensible Unternehmensdaten zugreifen und weitreichende Folgen für Datensicherheit und Compliance haben können. Da KI-Tools immer einfacher zugänglich und effizienter werden, nutzen Mitarbeiter sie zunehmend ohne Kontrolle durch die IT. Auch wenn dies auf den ersten Blick harmlos erscheint, entstehen dadurch Risiken, die herkömmliche Sicherheitsframeworks nicht allein durch ein Verbot von KI-Tools abfangen können.

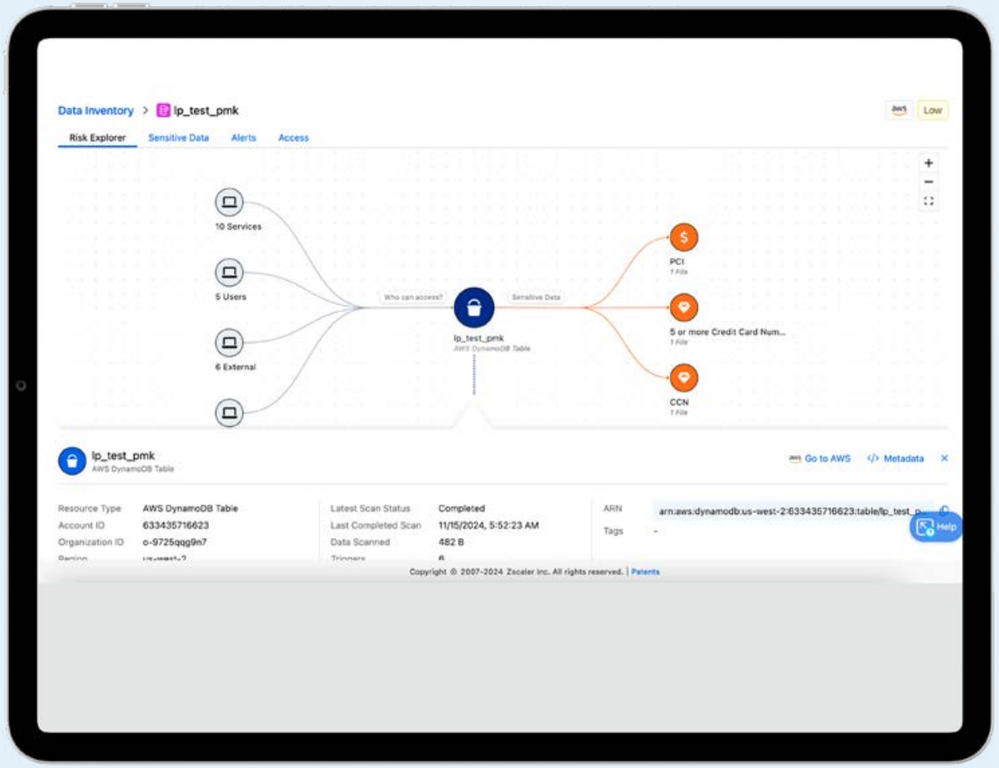
Mit DSPM können Unternehmen die Vorteile von KI voll ausschöpfen. Anstatt KI-Tools zu blockieren oder zu verbieten, können Unternehmen die Risiken von Schatten-KI mit DSPM steuern und gleichzeitig die Vorteile von KI nutzen. Mit der in DSPM integrierten Sicherheitsfunktion erhalten Teams einen vollständigen Überblick über Daten und KI-Modelle und können Risiken durch KI proaktiv verhindern. Damit können Sie folgendes erreichen:

- Lückenlose Übersicht über Ihre KI-Modelle, -Agenten und -Services
- Identifizieren und schützen Sie KI-Trainingsdaten vor Datenmanipulation, Fehlkonfigurationen und ungewollter Offenlegung
- Einhaltung und Umsetzung neuer KI-Compliance-Frameworks

Mithilfe von DSPM können Sicherheitsverantwortliche aus unübersichtlichen Sicherheitslandschaften kontrollierte Innovationen schaffen — mit zentraler Datenerfassung, kontextbasierter Risikoanalyse und automatisierter Governance für jede KI-Interaktion.

5. Ebenda.





KI-gestützte Datenklassifizierung

Effektive Datenklassifizierung ist ein grundlegender Aspekt einer robusten Datensicherheit. Wer sensible Daten proaktiv den jeweiligen Risiken zuordnet, kann potenzielle Gefahren durch Fehlkonfigurationen oder unsichere Abläufe gezielt vermeiden. Herkömmliche Ansätze, die oft auf manuellen Verfahren oder vereinfachter Mustererkennung beruhen, führen oft zu vielen Fehlalarmen und ineffizientem Einsatz von Sicherheitsressourcen. Viele Unternehmen setzen nach wie vor stark auf regexbasierte Lösungen — ein starrer Ansatz, der häufig Fehlalarme produziert und sich als brüchig und ineffizient erweist. Auch moderne Einzelprodukte schaffen es oft nicht, die Datenklassifizierung in eine zentrale Plattform zu integrieren, wodurch Warnmeldungen inkonsistent und die Transparenz fragmentiert bleibt, besonders wenn Daten durch das gesamte Unternehmensökosystem wandern.

Mit DSPM und der KI-gestützten LLM-Klassifizierung können Sicherheitsverantwortliche traditionelle Regex-Workflows ergänzen und erhalten so herausragende Transparenz und Flexibilität. So lassen sich sowohl bekannte als auch bisher unbekannte sensible Daten zuverlässig schützen. Im Gegensatz zu keywordbasierten Ansätzen erkennt die LLM-Klassifizierung Inhalte auf tieferer Ebene: Sie nutzt fortschrittliche Sprachverarbeitung, um den Kontext und die Intention zu erfassen, ohne auf vordefinierte Muster angewiesen zu sein. So können Unternehmen nicht nur bestehende Prozesse optimieren, sondern auch bisher verborgene sensible Daten identifizieren und schützen.

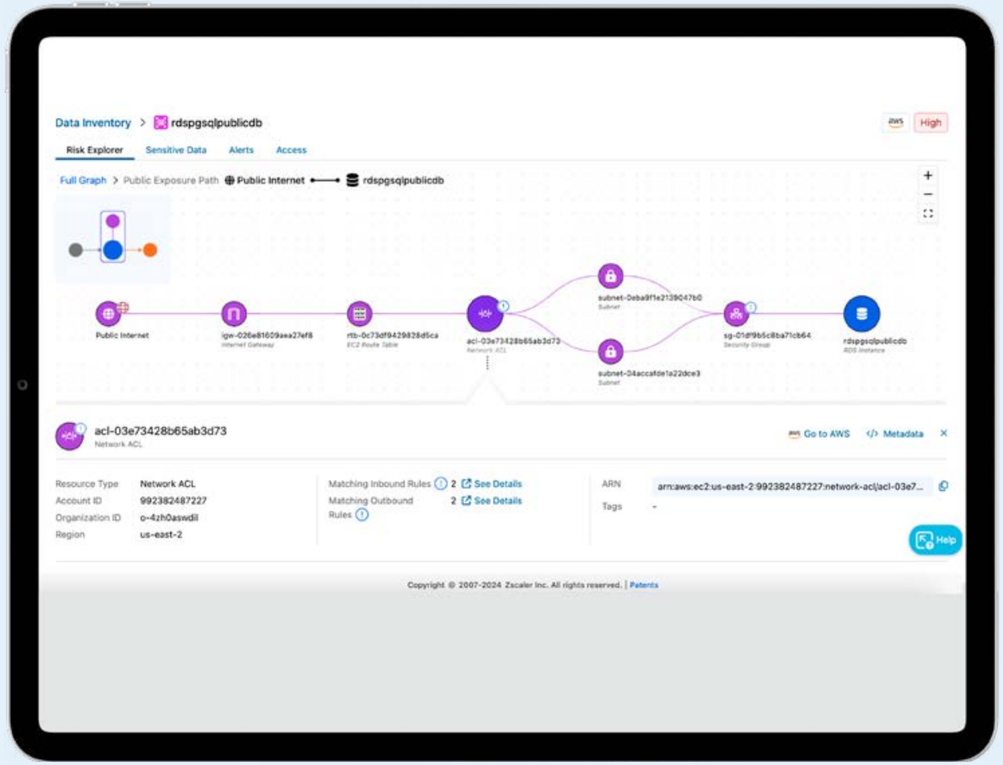
Proaktives Risikomanagement

Um Sicherheitsrisiken wirksam zu kontrollieren und die Einhaltung von Vorschriften zu gewährleisten, müssen Sicherheitsverantwortliche ihren Datensicherheitsstatus proaktiv verwalten. Eine der interessantesten Einsatzmöglichkeiten von KI in der Datensicherheit: proaktive Sicherheitsstrategien und prädiktive Analysen. Durch Analyse und Korrelation von Daten können KI-Algorithmen potenzielle Sicherheitsrisiken vorhersagen. Mit diesem proaktiven Ansatz können Unternehmen Bedrohungen und kritischen Risiken immer einen Schritt voraus bleiben.

Mit KI und fortschrittlichen Korrelationsmethoden erkennt DSPM Muster und Trends in Daten, die auf potenzielle Sicherheitsvorfälle hindeuten. Darüber hinaus können Datenbestände nach ihrem Wert (Risikostufe) priorisiert werden. So kann sichergestellt werden, dass sich Sicherheitsmaßnahmen auf die kritischsten Ressourcen konzentrieren. Außerdem verringert KI durch die Automatisierung zahlreicher Sicherheitsprozesse die Arbeitsbelastung der Sicherheitsexperten, ermöglicht einen proaktiven Sicherheitsansatz und verbessert die allgemeine Betriebseffizienz.

Beispielsweise kann die fortschrittliche Korrelationsfunktion von Zscaler DSPM Risiken proaktiv erkennen und versteckte Zusammenhänge aufdecken, sodass Sicherheitsmaßnahmen gezielt auf die kritischsten Daten konzentriert werden.

6. **IBM's Cost of a Data Breach Report 2025**



49 %

der Organisationen investieren nach einem Sicherheitsvorfall in die Sicherheit.[6]

Optimierte Compliance durch Echtzeit-Governance

Die Einhaltung von sich ständig ändernden Vorschriften und internen Sicherheitsprotokollen ist ein Eckpfeiler der KI- und Datensicherheit, von der DSGVO bis zur SEC. Heutzutage müssen Unternehmen nicht nur etablierte Vorschriften wie DSGVO und HIPAA einhalten, sondern auch neue Frameworks, die speziell auf KI abzielen, darunter das EU-Gesetz zur künstlichen Intelligenz, NIST AI 600 und ähnliche Vorgaben. Sicherheits- und Compliance-Risiken sind untrennbar miteinander verbunden. Sie beeinflussen sich gegenseitig grundlegend und prägen die Entwicklung eines Unternehmens. Verstöße gegen Sicherheitsvorgaben können nicht nur hohe Bußgelder nach sich ziehen, sondern auch das Vertrauen in Ihr Unternehmen erheblich beeinträchtigen. Umgekehrt kann die Einhaltung von Vorschriften auch als Schutzschild dienen und KI sowie Daten vor Sicherheitslücken und Bedrohungen schützen.

Viele Vorschriften lassen sich meist auf drei Grundprinzipien herunterbrechen: Kenntnis über KI und sensible Daten, Begrenzung des Zugriffs und kontinuierliche Risikoüberwachung. So einfach das klingt — die Komplexität von KI- und Datenumgebungen macht dies oft zu einer beträchtlichen Herausforderung. Darüber hinaus entwickeln sich die Vorschriften aufgrund neuer Technologien, veränderter Datenschutzbedenken und der zunehmenden Vernetzung der Weltwirtschaft ständig weiter. In einem sich ständig wandelnden regulatorischen Umfeld müssen Unternehmen dauerhaft wachsam bleiben und sich anpassen, um Compliance sicherzustellen. Herkömmliche Ansätze mit fragmentiertem Einblick, manuellen Überprüfungen und reaktiven Maßnahmen stoßen hier schnell an ihre Grenzen und liefern weder Klarheit noch Effizienz.

DSPM kann Compliance-Prozesse durch Daten-Compliance- und Governance-Funktionen in Echtzeit optimieren. Mit DSPM erhalten Unternehmen einen umfassenden Überblick über den Compliance-Status ihrer Daten, inklusive detaillierter Analysen, Benchmarking, Maßnahmen zur Behebung von Problemen und Reporting, um Compliance-Lücken schnell zu schließen. Besonders in stark regulierten Branchen ist ein klarer Einblick in Datenstatus und Maßnahmen zur Risikominderung entscheidend. Geführte Schritte zur Problemlösung und automatisierte Workflows helfen Sicherheitsteams, zügig und effektiv zu handeln. KI-gestützte Daten-Governance sorgt dafür, dass regulatorische Anforderungen eingehalten werden, ohne die Sicherheit zu vernachlässigen.

63%

der Organisationen haben keine KI-Governance-Richtlinien[7]

7. https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls

Das Prinzip der minimalen Rechtevergabe

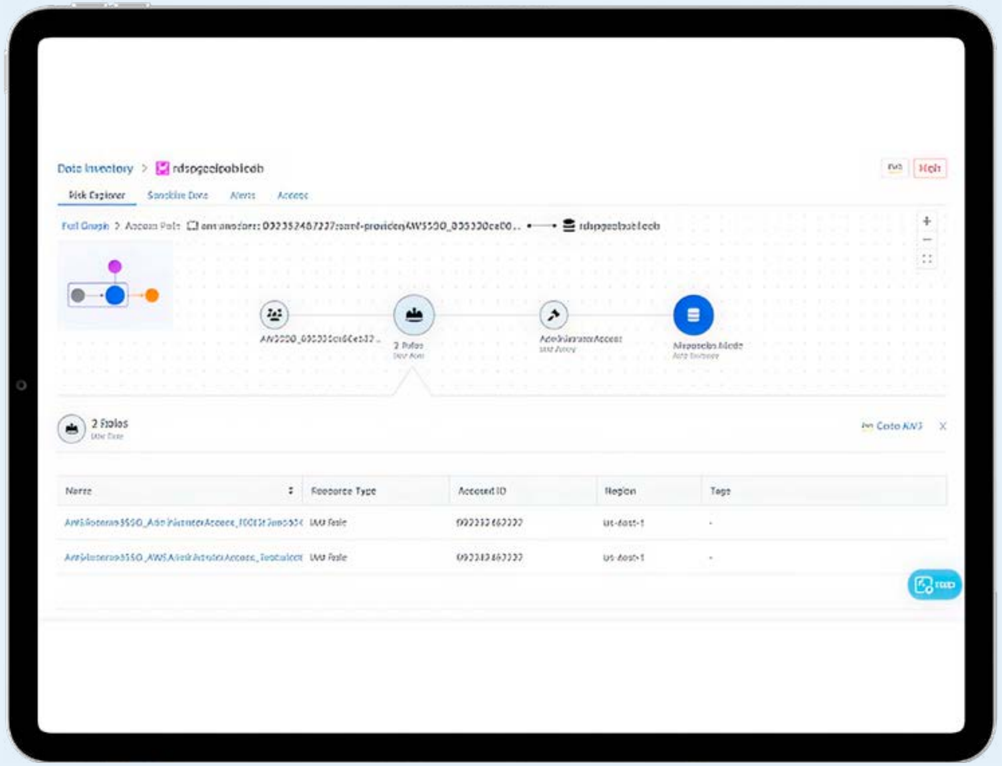
Durch die enorme Anzahl an Usern, Anwendungen und Ressourcen bergen Datenumgebungen ein hohes Risiko für unzureichende Zugriffskontrollen, ausufernde Useridentitäten und verwaiste Datenbestände. Rund 90 % aller Unternehmen erlitten bereits Sicherheitsvorfälle im Zusammenhang mit Identitäten — mit teuren Folgen.

Darüber hinaus bringen KI-Modelle und LLM-gestützte Tools zusätzliche Risiken in Hinblick auf unbefugten Datenzugriff mit sich. Zu den wichtigsten Gefahren zählen unbeabsichtigte oder unautorisierte Offenlegungen sensibler Daten, Datenexfiltration — also das Abgreifen sensibler Daten über KI-Ausgaben — sowie ausgeklügelte Angriffe, bei denen kompromittierte Identitäten KI-Systeme ausnutzen, um unbefugt Zugriff zu erhalten.

Aus diesem Grund gehört der Zugriff mit minimaler Rechtevergabe auf Datenspeicher zu den Grundpfeilern der Datensicherheit. Unübersichtliche Daten und Berechtigungen sowie komplexe KI- und Multicloud-Strukturen machen die Kontrolle über Zugriffsrechte allerdings zu einer Herausforderung. Trotzdem bleibt sie unverzichtbar, denn die unbefugte Offenlegung sensibler Daten ist häufig der Auftakt zu einem raffinierten Angriff.

DSPM liefert einen einheitlichen Ansatz für die Governance von Datenzugriffen und behält dabei kontinuierlich den Datensicherheitsstatus und das Verhalten der User im Blick. Das System analysiert Rollen, Berechtigungen und weitere Attribute im Identitäts- und Zugriffsmanagement, um gefährliche Zugriffspfade zu Datenspeichern frühzeitig aufzudecken. DSPM deckt strukturierte und unstrukturierte Daten ebenso ab wie On-Premise-, Multicloud- und SaaS-Umgebungen. So können Sie Zugriffsrisiken konsequent erkennen, Maßnahmen ergreifen und Richtlinien über Ihre gesamte Datenlandschaft und das KI-Ökosystem hinweg durchsetzen. Durch detaillierte Einblicke in Zugriffsmuster und mögliche Schwachstellen lassen sich minimale Zugriffsrechte noch besser durchsetzen, was das Risiko unbefugter Zugriffe reduziert und die Sicherheit Ihrer Datenumgebung insgesamt stärkt.

8. Security Today, Study: **90 Percent of Organizations Experienced an Identity-Related Incident in Last Year**, 5. Juni 2024.



90%

der Organisationen haben bereits einen Vorfall im Zusammenhang mit Useridentitätent erlebt.[8]

Speicher- und Verbrauchskosten optimieren

Datenteams müssen Speicher- und Nutzungskosten optimieren, indem sie doppelte oder verwaiste Datenspeicher erkennen, die gelöscht oder auf kostengünstigere Speicherlösungen verschoben werden können. Herkömmliche Methoden stoßen dabei oft an ihre Grenzen, was zu unnötigen Ausgaben führt.

DSPM-Lösungen können zur Lösung dieses Problems beitragen, indem sie Einblicke in doppelte oder verwaiste Datenspeicher liefern, sodass Unternehmen entsprechende Maßnahmen ergreifen können. Zscaler DSPM bietet eine umfassende Übersicht über doppelte oder verwaiste Datenspeicher und unterstützt die zuständigen Teams beim Erkennen von Daten, die sicher gelöscht oder migriert werden können.

Mithilfe KI-gestützter Erkenntnisse können Unternehmen unnötige Speicherkosten senken und die ordnungsgemäße Verwaltung und den Schutz vertraulicher Informationen sicherstellen.

Einheitliche Richtlinien für alle Datenumgebungen

Mit herkömmlichen Methoden stellt die Aufrechterhaltung konsistenter Datensicherheitsrichtlinien in unterschiedlichen Umgebungen eine gewaltige Herausforderung dar. Mit DSPM-Lösungen können Sie diese Herausforderung bewältigen, indem Sie einen einheitlichen Ansatz für die Datensicherheit in Multicloud-Umgebungen nutzen und einheitliche Richtlinien in allen Datenumgebungen durchsetzen.

Zscaler DSPM gewährleistet eine einheitliche Datensicherheitsstrategie. Damit haben Sie die Möglichkeit, einheitliche Richtlinien für alle Datenumgebungen festzulegen, eine umfassende Überwachung der Cloud-Daten sicherzustellen und den Prozess der Risikoerkennung und -behebung zu optimieren. Durch Nutzung KI-gestützter Erkenntnisse können Sie das Risiko von Datenpannen verringern und Datenschutzvorschriften besser einhalten.

Schnelle Reaktion auf Sicherheitsvorfälle

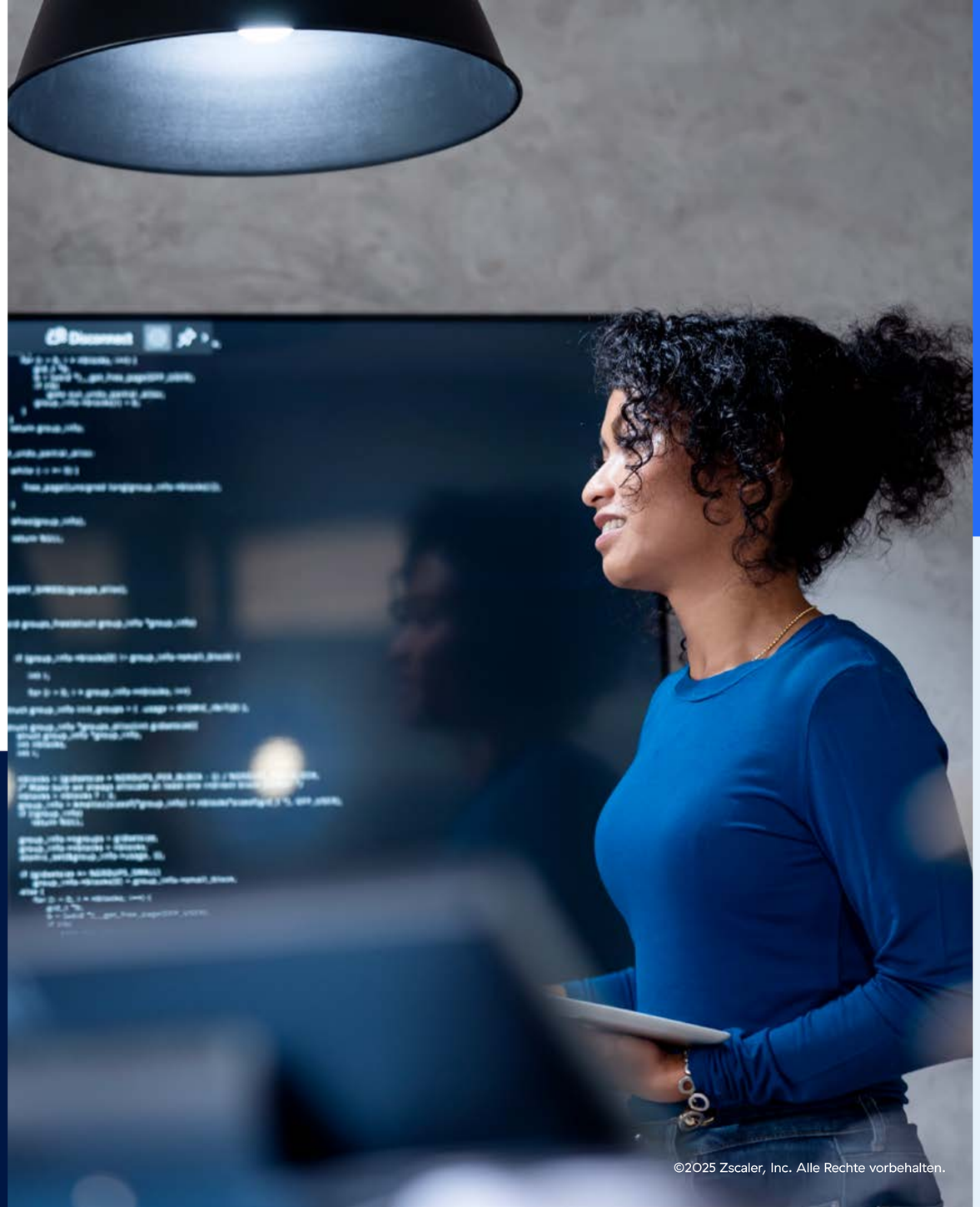
Risiken frühzeitig zu erkennen und zu minimieren, ist die Kernaufgabe von Sicherheitsteams. Da sich Bedrohungen immer schneller weiterentwickeln, müssen Sie in Echtzeit reagieren können. Konventionelle Methoden kommen dabei oft nicht mit, insbesondere in einer dynamischen KI-basierten Bedrohungsumgebung. Hier setzt KI-gestützte Sicherheitsautomatisierung an.

Mit DSPM behalten Sie Ihre Daten kontinuierlich im Blick, erkennen Auffälligkeiten frühzeitig und können schneller auf Bedrohungen reagieren. DSPM-Lösungen unterstützen Sie bei der Risikominderung durch intelligente Risiko-Korrelationen und adaptive Zugriffsinformationen. Bestimmte Lösungen, wie Zscaler DSPM, kombinieren ThreatLabz-Bedrohungsinformationen mit präzisen, geführten Behebungsmaßnahmen und einer schnellen Umsetzung von Sicherheitsmaßnahmen. Durch KI-gestützte Bedrohungskorrelation lassen sich verborgene Risiken und zentrale Angriffspunkte aufdecken, sodass Sie sich auf die wirklich kritischen Gefahren konzentrieren können.

9. Statista, **Mean time to identify and contain data breaches worldwide from 2017 to 2024**, aufgerufen am 9. Dezember 2024.

194 Tage

Die durchschnittliche Zeit zur Erkennung einer Datenpanne[9]



Verbesserte KI-Sicherheit

Unternehmen setzen KI-Anwendungen in rasantem Tempo ein. Dabei erhöhen besonders generative KI (GenAI) und Large Language Models (LLMs) das Risiko von Datenpannen und Compliance-Verstößen. Laut einem aktuellen Report haben 13 % der Organisationen bereits Sicherheitsvorfälle im Zusammenhang mit KI-Modellen oder -Anwendungen gemeldet[10] — ein deutlicher Hinweis darauf, dass KI zu einem attraktiven Ziel für Cyberkriminelle wird.

Unternehmen, die GenAI in ihre Betriebsabläufe integrieren, müssen Maßnahmen ergreifen, um die unbeabsichtigte Verwendung vertraulicher Daten innerhalb dieser Modelle zu verhindern. Sicherheitsteams müssen Daten kennzeichnen, taggen und klassifizieren, damit alle Teams GenAI sicher und verantwortungsvoll einsetzen können.

Mit DSPM lässt sich die Kontrolle und Absicherung von Daten in GenAI-Umgebungen durch integrierte KI-SPM-Funktionen deutlich verbessern. Indem Daten präzise erkannt und kategorisiert werden, verhindert DSPM, dass sensible Informationen an LLMs gelangen, und senkt so das Risiko von Datenpannen und Compliance-Verstößen. DSPM setzt auf einen „Data-First"-Ansatz: Die Lösung schützt die Informationen, die die KI verwendet, statt nur die zugrunde liegende Infrastruktur. Durch kontinuierliches Erkennen, Klassifizieren und Überwachen von Daten über ihren gesamten Lebenszyklus hinweg unterstützt DSPM dabei, spezielle KI-Sicherheitsrisiken wie Datenmanipulation, die Offenlegung sensibler Daten oder den Diebstahl von Modellen zu minimieren.

Mit DSPM, das über integrierte KI-SPM-Funktionen verfügt, können Unternehmen Vertrauen in ihre KI-Anwendungen schaffen. Gleichzeitig schützen sie ihre wertvollen Daten und sorgen dafür, dass KI-Anwendungen stabiler und sicherer laufen.

10. https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls

DSPM zur Absicherung einer vielfältigen Datenlandschaft

Der strategische Einsatz von KI und DSPM ist für die Verbesserung der Datensicherheit von entscheidender Bedeutung. Diese Technologien bieten den erforderlichen Kontext und die Automatisierung, um die Komplexität moderner Datenumgebungen effektiv zu bewältigen. Indem Sicherheitsteams proaktiv vorgehen, können sie sensible Daten effektiv absichern, Vorschriften einhalten und die Risiken fortschrittlicher Technologien wie GenAI mindern.

„Bis 2026 werden mehr als 20 % der Unternehmen DSPM-Technologien implementieren, da es unerlässlich ist, bisher unbekannte Datenspeicher zu erkennen und zu lokalisieren und die damit verbundenen Sicherheits- sowie Datenschutzrisiken zu minimieren."

Gartner, Innovation Insight: Data Security Posture Management,
Brian Lowans, Joerg Fritsch, Andrew Bales, 28. März 2023

Zscaler DSPM

Zscaler DSPM ist die weltweit umfassendste integrierte Plattform zum Schutz strukturierter und unstrukturierter Daten in SaaS-, öffentlichen Cloud- (AWS, Azure, GCP) und On-Premise-Umgebungen sowie auf Endgeräten.

Die Lösung bietet einen detaillierten Einblick in Ihre Cloud-Daten, klassifiziert und identifiziert Daten sowie Zugriffe und kontextualisiert Datenexposition und Sicherheitsstatus. So können Unternehmen und Sicherheitsbeauftragte Datenpannen in der Cloud auch bei hohen Volumen verhindern und beheben.

Zscaler DSPM verfolgt einen KI-gestützten, einheitlichen Ansatz, um eine hohe Datenhygiene in allen Datenspeichern zu gewährleisten, einschließlich IaaS, SaaS, On-Premise, Endgeräte und mehr. Durch die native Integration in die Zscaler Data Security Platform erhalten Sie einen vollständigen Überblick und uneingeschränkte Kontrolle über Ihre Daten auf einer zentralen Plattform.

Mit einer einzigen, einheitlichen DLP-Engine bietet die Zscaler Data Security Platform konsistenten und erstklassigen Schutz für Ihre Daten auf allen Kanälen. Indem alle User an allen Standorten überwacht und Daten sowohl bei der Übertragung als auch im Ruhezustand kontrolliert werden, gewährleistet die Plattform den nahtlosen Schutz sensibler Daten und die Einhaltung von Compliance-Vorgaben.

Weitere Informationen finden Sie unter zscaler.com/de/dp/dspm.

Interaktive Produktdemo von DSPM starten

Warum ist DSPM eine wichtige Komponente Ihrer Data Protection-Strategie?

On-demand-Webinar ansehen ⟶

Scannen Sie den QR-Code, um auf hilfreiche DSPM-Ressourcen zuzugreifen:

zscaler™ | Experience your world, secured.™

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die Zscaler Zero Trust Exchange™ schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlusten. Als weltweit größte Inline-Cloud-Sicherheitsplattform wird die SASE-basierte Zero Trust Exchange™ in über 150 Rechenzentren auf der ganzen Welt bereitgestellt. Weitere Informationen erhalten Sie auf **www.zscaler.com/de**. Auf X (ehemals Twitter) finden Sie uns unter **@zscaler**.

+1 408 533 0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA zscaler.com/de