Schutz für Cloud-Daten und Verhinderung von Datenpannen mit Zscaler DSPM

Einmal definieren, überall anwenden — mit der weltweit umfassendsten, vollständig integrierten Data Protection-Plattform

Cloud-Daten sind das neue Ziel

82 %

82 % der Datenpannen betrafen Daten, die in Cloud-Umgebungen gespeichert waren

227

Die durchschnittliche Zeit, bis eine Datenpanne erkannt wird, beträgt 227 Tage

4,45 Mio.

Die Kosten einer Datenpanne belaufen sich durchschnittlich auf 4,45 Millionen US-Dollar.

„STATE OF DATA GOVERNANCE AND EMPOWERMENT REPORT" ESG, 2022
„COST OF A DATA BREACH 2023 REPORT" IBM SECURITY, 2023

„Bis 2026 werden mehr als 20 % der Unternehmen DSPM-Technologie [Data Security Protection Management] implementieren, da es dringend erforderlich ist, bisher unbekannte Datenspeicher zu erkennen und zu lokalisieren und die damit verbundenen Sicherheits- sowie Datenschutzrisiken zu minimieren."

– Gartner

GARTNER UNTERSTÜTZT KEINE ANBIETER, PRODUKTE ODER DIENSTLEISTUNGEN, DIE IN SEINEN FORSCHUNGSPUBLIKATIONEN AUFGEFÜHRT SIND, UND EMPFIEHLT TECHNOLOGIEANWENDERN NICHT, NUR ANBIETER MIT DEN HÖCHSTEN BEWERTUNGEN AUSZUWÄHLEN. PUBLIKATIONEN VON GARTNER SPIEGELN DIE ANSICHTEN VON GARTNERS FORSCHUNGSORGANISATION WIDER UND SOLLTEN NICHT ALS TATSACHENFESTSTELLUNGEN INTERPRETIERT WERDEN. GARTNER ÜBERNIMMT KEINERLEI GEWÄHRLEISTUNG, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND, IN BEZUG AUF DIESE FORSCHUNG SOWIE FÜR DIE MARKTTAUGLICHKEIT ODER EIGNUNG DER GENANNTEN PRODUKTE FÜR EINEN BESTIMMTEN ZWECK.

Herausforderungen bei der Absicherung von Daten in einer cloudzentrierten Welt

Multicloud-Umgebungen sind zwangsläufig komplex und ressourcenintensiv. Die riesige Menge an Daten, die in die Cloud verschoben wird, und die hohe Anzahl von Usern, die auf verschiedene Cloud-Plattformen, -Konten und -Services zugreifen, erschwert es Unternehmen, die Vorgänge in der Cloud zu überblicken und zu kontrollieren.

Sicherheitsexperten stehen beim Schutz von Daten in einer Multicloud-Umgebung vor vier großen Herausforderungen:

1 DIE CLOUD IST AGIL

Moderne, agile Cloud-Technologien und -Services bieten Entwicklern die Flexibilität, problemlos zusammenzuarbeiten und Daten auszutauschen, was zu einem Verlust an Transparenz und Kontrolle über sensible Daten führen kann.

2 DIE CLOUD IST KOMPLEX

Schätzungsweise wird die Gesamtmenge der Cloud-Daten bis 2025 von heute 33 ZB auf 175 ZB ansteigen. Angesichts des ausufernden Datenwachstums in mehreren Cloud-Plattformen, -Konten und -Services haben Unternehmen Schwierigkeiten nachzuvollziehen, welche Cloud-Services, -Regionen und -Konten Daten verbrauchen und speichern.

3 ÜBERMÄSSIGE BERECHTIGUNGEN

Zusätzlich zu den Herausforderungen bei der Erkennung und Klassifizierung von Daten haben Sicherheitsteams auch Schwierigkeiten, den Datenzugriff zu überblicken und gleichzeitig die Vorgaben zur Datensouveränität zu erfüllen, was zu massiven Sicherheitslücken führt.

4 FEHLENDER DATENKONTEXT

Eine Flut von Warnmeldungen zu Fehlkonfigurationen und Schwachstellen ohne Priorisierung auf der Grundlage des Kontexts sensibler Daten führt zur Überlastung der Ressourcen und zu Sicherheitsverstöße.

Welche Faktoren treiben die Nachfrage nach umfassenden CSPM-Lösungen an?

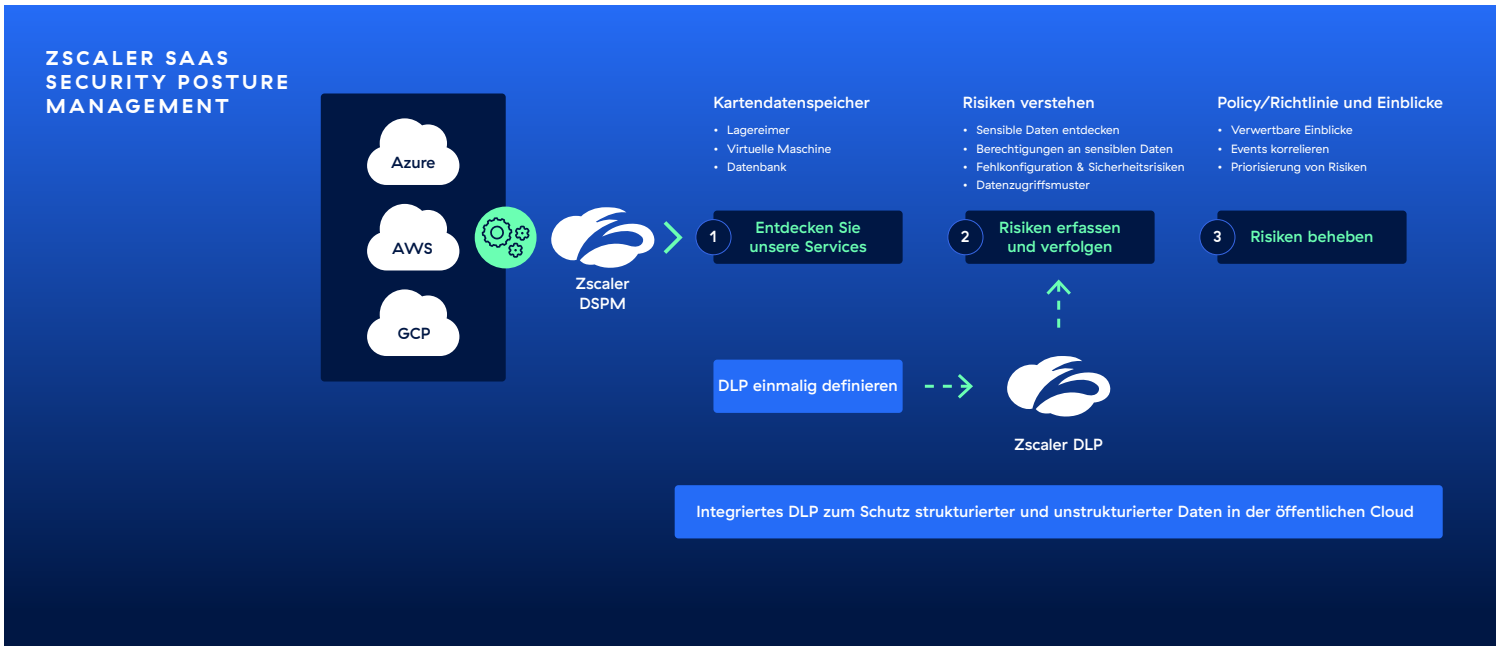
Leider hat sich gezeigt, dass herkömmliche Data Protection-Lösungen nicht für dynamische Multicloud-Umgebungen geeignet sind. Gleichzeitig stellen einzelne DSPM-Anbieter isolierte Ansätze bereit, die sich nicht nahtlos in bestehende Data Protection-Programme integrieren lassen. Es ist offensichtlich, dass Unternehmen einen neuen, einheitlichen Ansatz zur Absicherung ihrer Cloud-Daten benötigen.

Ein Überblick über Zscaler Data Security Posture Management (DSPM)

Zscaler AI Data Protection ist die weltweit umfassendste vollständig integrierte Data Protection-Plattform, die sowohl strukturierte als auch unstrukturierte Daten im Web, in SaaS-basierten Services, öffentlichen Cloud-Umgebungen (AWS, Azure, GCP), privaten Anwendungen, E-Mails und auf Endgeräten schützt.

Als Teil der Zscaler-Plattform erweitert Zscaler Data Security Posture Management (DSPM) die robuste, erstklassige Sicherheit für Ihre Daten auf die öffentliche Cloud. DSPM bietet einen detaillierten Einblick in Ihre Cloud-Daten, klassifiziert und identifiziert Daten sowie Zugriffe und kontextualisiert Datenexposition und Sicherheitsstatus. So können Unternehmen und Sicherheitsteams Datenpannen in der Cloud in großem Maßstab verhindern und beheben.

Die Lösung verwendet eine einzige und einheitliche DLP-Engine, um konsistente Data Protection über alle Kanäle hinweg zu gewährleisten. Durch die Überwachung aller User an allen Standorten und die Kontrolle der Daten während der Nutzung und im Ruhezustand wird sichergestellt, dass sensible Daten nahtlos geschützt werden und die Compliance eingehalten wird.



Warum Zscaler DSPM?

1 EINE EINHEITLICHE DATENSICHERHEITSPLATTFORM

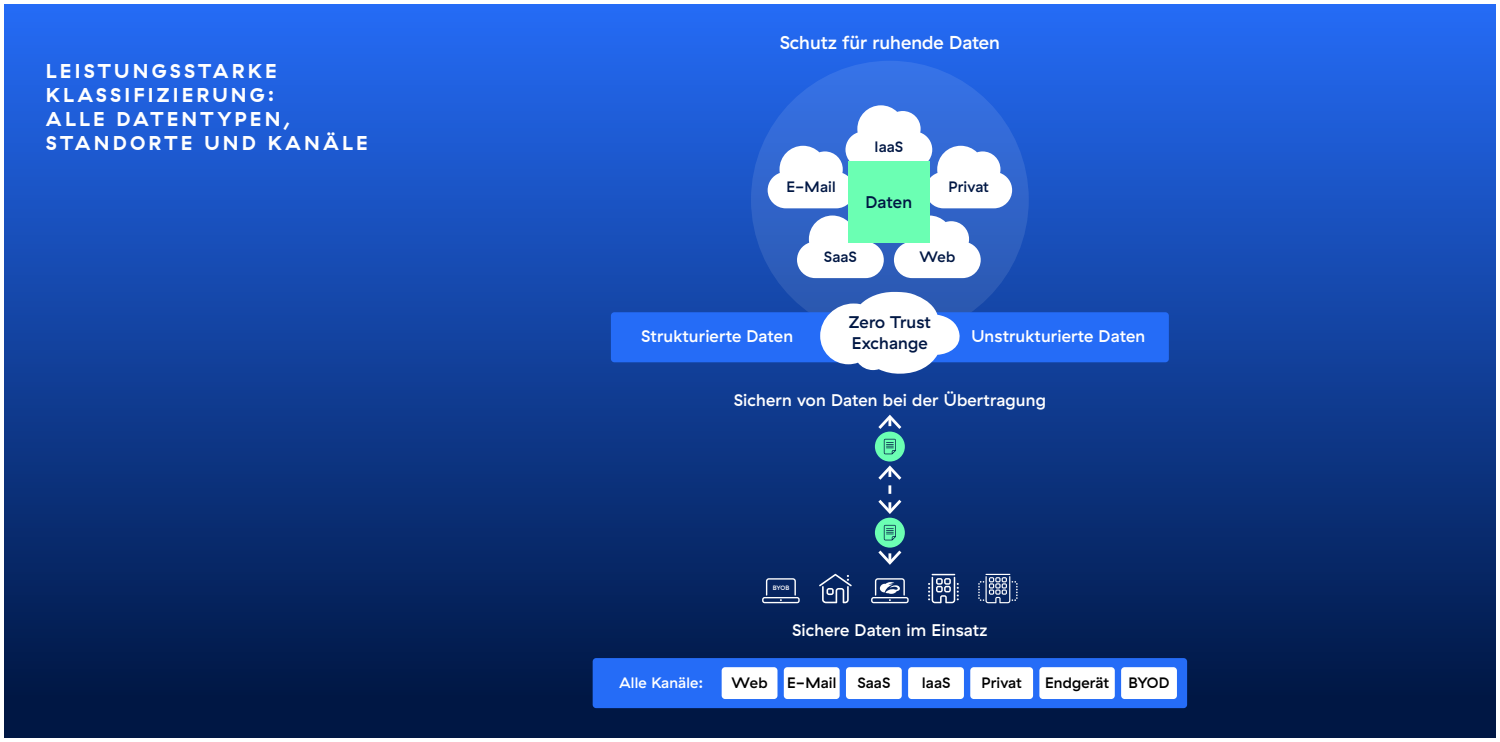
Zscaler DSPM lässt sich nahtlos mit der Zscaler-AI-Data-Protection-Plattform integrieren, die speziell mit einer zentralen DLP-Engine entwickelt wurde, mit der Sicherheitsteams optimale Datensicherheit für Web, SaaS, On-Premise-Anwendungen, Endgeräte, BYOD-Geräte und die öffentliche Cloud erzielen können.

2 AUTOMATISCHE DATENERKENNUNG MIT KI

Erkennen, klassifizieren und identifizieren Sie Daten automatisch und ohne Konfiguration, während Sie Bereitstellung und Betrieb mit einem agentlosen Ansatz deutlich beschleunigen.

3 EFFIZIENTERE TEAMS UND VEREINFACHTE ABLÄUFE

Die leistungsstarke Bedrohungskorrelation, die versteckte Risiken und kritische Angriffspfade aufdeckt, reduziert die Überlastung durch Warnmeldungen erheblich, sodass sich Ihr Team auf die Risiken konzentrieren kann, die am wichtigsten sind.



DSPM: Anwendungsfälle

FUNKTION	VORTEIL	GESCHÄFTSNUTZEN
Datenerkennung und -klassifizierung	Scannen und erkennen Sie sensible Daten auf verschiedenen Cloud-Plattformen und -Services in Echtzeit oder nahezu in Echtzeit. Kategorisieren, kennzeichnen und inventarisieren Sie sensible Daten auf der Grundlage von vordefinierten oder userdefinierten Richtlinien genau. Erhalten Sie präzise, KI-basierte Datenklassifizierung, die von der Zscaler-Plattform unterstützt wird, die täglich Milliarden von Transaktionen überwacht.	Verschaffen Sie sich einen exklusiven Einblick in die Datenflut in der Cloud und erkennen Sie sensible Daten — selbst an unbekannten Speicherorten.
Ermitteln und Nachverfolgen von Gefährdungen	Verschaffen Sie sich einen einheitlichen Überblick über Sicherheit, Inventar und Compliance für sensible Daten in Ihrer Multicloud-Umgebung. Erhalten Sie einen granularen, risikobasierten, userzentrierten Überblick über alle Zugriffspfade auf unternehmenskritische Datenbestände und deren Konfiguration. Analysieren Sie versteckte Risiken wie Fehlkonfigurationen, übermäßige Berechtigungen und Schwachstellen.	Informieren Sie sich über die Auswirkungen kompromittierter Datenbestände, den Zugriff, versteckte Angriffspfade und aktuelle komplexe Bedrohungen.
Risikobehebung	Priorisieren Sie die Risiken nach Schweregrad. Beheben Sie Probleme und Verstöße mithilfe kontextbasierter, geführter Abhilfemaßnahmen direkt an der Quelle.	Minimieren Sie das Risiko von Datenexposition und Datenpannen.
Konsistenter Sicherheitsstatus	Sorgen Sie überall für konsistente, erstklassige Datensicherheit, von Endgeräten bis hin zu E-Mail, SaaS, öffentlicher Cloud usw.	Verbessern Sie den allgemeinen Sicherheitsstatus und seien Sie Bedrohungen einen Schritt voraus.
Kontinuierliche Compliance-Berichterstattung	Gleichen Sie Ihren Sicherheitsstatus laufend mit den gesetzlichen Vorgaben ab, um Compliance-Verstöße zu erkennen und zu beheben. Nutzen Sie ein umfassendes Compliance-Dashboard, das die sicherheitsbezogene Zusammenarbeit zwischen abteilungsübergreifenden Teams vereinfacht.	Überwachen Sie Verstöße, vereinfachen Sie Audits und verhindern Sie finanzielle Verluste und Imageschäden.
Workflow-Integration	Sie können die Lösung nahtlos in Ihr bestehendes Sicherheits-Ökosystem, in Services von Drittanbietern, in native Tools zur Risikopriorisierung und in Anwendungen für die Zusammenarbeit im Team integrieren.	Minimieren Sie Kosten und Komplexität der Absicherung vertraulicher Daten.

Schlüsselkomponenten von Zscaler DSPM

Datenerkennung	Erkennt strukturierte und unstrukturierte Datenspeicher	In der DSPM-SKU enthalten
Datenklassifizierung	Automatische Erkennung und Klassifizierung sensibler Daten mit vorkonfigurierter Erkennung und benutzerdefinierten Regeln	In der DSPM-SKU enthalten
Datenzugriffskontrolle	Erfasst und verfolgt den Zugriff auf Datenressourcen	In der DSPM-SKU enthalten
Risikobewertung	Erkennt und priorisiert Risiken basierend auf Schweregrad und Auswirkung mithilfe von KI, ML und erweiterter Bedrohungskorrelation	In der DSPM-SKU enthalten
Risikobehebung	Bietet eine schrittweise Anleitung zur Behebung mit vollständigem Kontext	In der DSPM-SKU enthalten
Compliance-Management	Gleicht den Sicherheitsstatus von Daten automatisch mit Branchen-Benchmarks und Compliance-Standards wie DSGVO*, CIS, NIST und PCI DSS* ab	In der DSPM-SKU enthalten

* PRODUKT-ROADMAP-FUNKTIONEN

Zscaler DPSM in der Praxis erleben

Demo vereinbaren

Die Vorteile der Zscaler-DSPM-Plattform lassen sich am besten im Rahmen einer Demo veranschaulichen.

DEMO ANFORDERN

Event zur Markteinführung ansehen

Überzeugen Sie sich selbst von den leistungsstarken Funktionen unserer Lösung und erleben Sie, wie DSPM zur Reduzierung von Komplexität beiträgt, Daten zuverlässig vor komplexen Angriffen und Cyberbedrohungen schützt und die Effizienz Ihres Sicherheitsteams optimiert.

EVENT ZUR MARKTEINFÜHRUNG ANSEHEN

Weitere Informationen finden Sie unter
www.zscaler.de/dspm