

Zscaler Data Security Posture Management (DSPM)

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Lösungsprofil

Überblick: Datensicherung in der Cloud-zentrierten Wirtschaft

Zu den Herausforderungen bei der Sicherung großer Mengen von Geschäftsdaten in Multicloud-Umgebungen gehören die effiziente Verwaltung komplexer und umfangreicher Bestimmungen für Data Protection, der Umgang mit Insider-Bedrohungen, Datenschutzverletzungen, Zugriffsberechtigungen für Drittuser und Lieferanten, Risiken in der Lieferkette sowie die Einhaltung aufsichtsrechtlicher Vorschriften. Unternehmen haben Schwierigkeiten, kritische Datenbestände zu inventarisieren, zu klassifizieren, zu kontrollieren und vor verschiedenen Bedrohungen zu schützen. Diese Komplexität wird durch eine Vielzahl fragmentierter Datenspeicherorte, Rollen und Berechtigungen in unterschiedlichen Umgebungen noch verstärkt.

Komplexe Umgebungen	Datenvolumen	Gezielte, komplexe Angriffe	Unnötige Zugriffsberechtigungen
82 % aller Datenpannen betreffen Cloud-Daten[1]	Geschätzte 175 ZB Daten werden 2025 in der Cloud gespeichert[2]	4,88 Mio. USD — die weltweiten Durchschnittskosten eines Datenschutzverstoßes im Jahr 2024[3]	80 % der Unternehmen waren Opfer von Identitätsdiebstählen[4]

Herkömmliche Data Protection-Lösungen sind den Anforderungen dynamischer Multicloud-Umgebungen nicht gewachsen. DSPM-Anbieter stellen isolierte Ansätze bereit, die sich nicht nahtlos in bestehende Data Protection-Programme integrieren lassen. Zur Bewältigung dieser Herausforderungen benötigen Unternehmen einen neuen, einheitlichen Ansatz zur Absicherung ihrer Cloud-Daten.

Zscaler löst diese Datensicherheitsprobleme in Multicloud-Umgebungen mit einer komplett integrierten DSPM-Lösung (Data Security Posture Management).

Was ist DSPM?

„Data Security Posture Management (DSPM) gibt Aufschluss darüber, wo sich Ihre vertraulichen Daten befinden, wer Zugriff auf diese Daten hat, wie sie verwendet wurden und wie es um den Sicherheitsstatus der gespeicherten Daten bzw. der betreffenden Anwendung bestellt ist.“ — Gartner

DSPM wird manchmal als „Data First“-Sicherheit bezeichnet und stellt quasi eine Umkehrung des gängigen Schutzmodells anderer Cybersicherheitstechnologien und -praktiken dar. Anstatt die Geräte, Systeme und Anwendungen zu sichern, die Daten speichern, verschieben oder verarbeiten, zielt DSPM auf den direkten Schutz der Daten ab und ergänzt damit andere Lösungen im Security-Stack eines Unternehmens.

DSPM umfasst insbesondere die kontinuierliche Überwachung, Überprüfung und Optimierung von Sicherheitskontrollen zum Schutz vertraulicher Daten auf verschiedenen Multicloud-Plattformen. Indem DSPM die Erkennung vertraulicher Daten, damit verbundener potenzieller Schwachstellen, Konfigurationsfehler und Compliance-Verstöße automatisiert, unterstützt die Lösung einen proaktiven Umgang mit dem Risiko einer Datenexposition. Auf diese Weise hilft DSPM Unternehmen, den allgemeinen Datensicherheitsstatus zu stärken, das Risiko von Datenschutzverletzungen zu minimieren und aufsichtsrechtliche Vorschriften zu erfüllen.

1. https://www.informationweek.com/cyber-resilience/data-breaches-just-keep-piling-up
2. https://www.forbes.com/sites/tomcoughlin/2018/11/27/175-zettabytes-by-2025/
3. https://www.ibm.com/reports/data-breach
4. https://www.darkreading.com/cybersecurity-operations/identity-related-breaches-last-12-months

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Warum DSPM?

Der Fokus von DSPM-Tools liegt auf der Bewertung und Verbesserung des Sicherheitsstatus der Datenumgebung eines Unternehmens durch Auffinden von Schwachstellen, Überwachen von Sicherheitseinstellungen und Erkennen potenzieller Bedrohungen für vertrauliche Daten. Über die bloße Durchsetzung von Richtlinien hinaus gibt DSPM Auskunft über den tatsächlichen Ist-Zustand der Unternehmensdaten.

Durch das Scannen und Kategorisieren von Daten erhalten Unternehmen einen umfassenden Überblick darüber, wo sich vertrauliche Daten befinden und wie sie verwendet werden. Darüber hinaus hilft eine DSPM-Lösung bei der Priorisierung der erkannten Probleme und verhindert eine Flut von Warnmeldungen, die dazu führen könnten, dass solche Probleme übersehen werden.

Zu den praktischen Anwendungsfällen von DSPM gehören das Erkennen von Sicherheitslücken (wie etwa Verschlüsselung) in Cloud-Umgebungen, das Durchsetzen von Zugriffsrichtlinien und die Bereitstellung von Warnmeldungen und Untersuchungsfunktionen für das Vorfallmanagement.

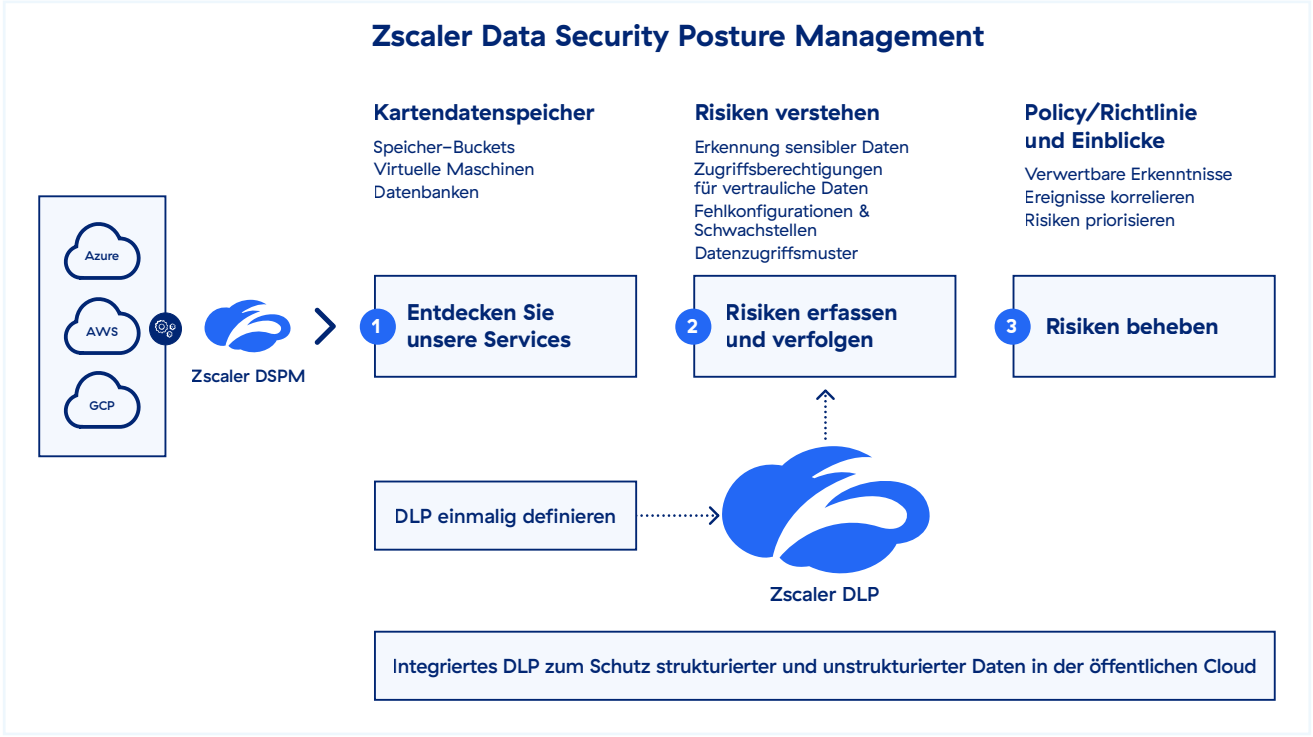
Wir stellen vor: Zscaler DSPM

Zscaler AI Data Protection ist die komplett integrierte Data Protection-Plattform mit dem weltweit größten Funktionsumfang. Die Lösung schützt strukturierte und unstrukturierte Daten im Web, in SaaS-basierten Services, öffentlichen Cloud-Umgebungen (AWS, Azure, GCP), privaten Unternehmensanwendungen, E-Mails und auf Endgeräten.



Als Modul der Zscaler-Plattform erweitert Zscaler DSPM robuste, erstklassige Datensicherheit in die öffentliche Cloud. Es bietet detaillierte Einblicke in Cloud-Daten, klassifiziert und erkennt Daten und Zugriffe und liefert Kontextinformationen zu Datenexposition und Sicherheitsstatus. So können Sicherheitsteams Cloud-Datenverletzungen auch bei hohen Volumen verhindern und beheben.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.



Mithilfe einer einzigen, einheitlichen DLP-Engine gewährleistet Zscaler DSPM konsistente Data Protection über alle Kanäle hinweg. 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.

Kernfunktionen von Zscaler DSPM

Datenermittlung, -klassifizierung und -inventar
Herkömmliche Scanmethoden sind teuer und erfordern erheblichen Aufwand, um verwertbare Ergebnisse zu erzielen. Zscaler DSPM scannt mit minimalem Zugriff auf Ressourcen in Cloud-Umgebungen (AWS, Azure und GCP) Datenspeicher, ermittelt vertrauliche Daten und klassifiziert Daten präzise. Die Lösung unterstützt eine Reihe von Anwendungsfällen:

- **Umfassende Datenermittlung:** Zscaler DSPM überwacht ständig Cloud-Umgebungen, um automatisch neue Datenspeicher zu erkennen, wenn diese in dynamischen Datenumgebungen instanziiert werden. So sparen Sie Zeit und vermeiden Transparenzlücken.
- **Präzise Datenklassifizierung:** Zscaler DSPM verwendet vordefinierte DLP-Engines und Wörterbücher zur Datenklassifizierung. Es bietet Einblick in die Art der in Cloud-Ressourcen gespeicherten vertraulichen Daten, die Region, die Dateien mit vertraulichen Daten, den Schweregrad des einschlägigen Risikos usw. Zudem haben Unternehmen auch die Flexibilität, die Richtlinien neu zu erstellen oder vorhandene Richtlinien zu replizieren.
- **Zuverlässige Inventarisierung:** Durch genaue Zuordnungen und Inventarlisten der Datenbestände können Sicherheitsbeauftragte vertrauliche Daten mühelos lokalisieren und nachvollziehen, wer Zugriff auf sie hat und wie sie verwendet werden.

Mit Zscaler DSPM erhalten Sicherheitsbeauftragte mehr Einblick in die Daten innerhalb der Cloud-Infrastruktur. Dadurch wird die Verwaltung und Verbesserung des Datensicherheitsstatus von Multicloud-Umgebungen, die komplexe Ebenen von SaaS, PaaS, IaaS und Datenbanken umfassen, wesentlich einfacher.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Datenexpositionen zuordnen und verfolgen

Cloud-Dienste und -Konfigurationen ändern sich häufig, was zu unbeabsichtigten und riskanten Datenexpositionen führen kann. Diese Sicherheitslücken müssen unbedingt geschlossen werden, bevor böswillige Akteure sie ausnutzen können. Zscaler DSPM erkennt öffentlich zugängliche Ressourcen sowie Schwachstellen oder Fehlkonfigurationen in den verschiedenen Komponenten (Netzwerksicherheitsgruppe, Load Balancer, virtuelles Netzwerk usw.), die mit der Datenressource verknüpft sind. Dadurch werden verschiedene Sicherheitsmaßnahmen unterstützt:

- **Analyse der Exposition:** Ermitteln Sie öffentliche Exposition, Fehlkonfigurationen und Schwachstellen bei Datenspeichern und -services.
- **Risikobewertung:** Aggregieren Sie das Gesamtrisikoniveau, indem Sie Auswirkung und Wahrscheinlichkeit kombinieren. Dabei werden Risiken in die Stufen hoch, mittel und niedrig eingeteilt.
- **Risikopriorisierung:** Unterstützen Sie Sicherheitsbeauftragte dabei, Alarmmüdigkeit zu vermeiden und Vorfälle basierend auf Risiko und Schweregrad zu priorisieren.
- **Erweiterte Bedrohungskorrelation:** Korrelieren Sie Bedrohungen, Risikofaktoren und versteckte Angriffspfade, um das Risiko zu minimieren.
- **Adaptive Zugriffsinformationen:** Erhalten Sie eine detaillierte, risikobasierte und userzentrierte Ansicht aller Zugriffspfade auf unternehmenskritische Daten und Konfigurationen.

Risikobehebung

Zscaler DSPM optimiert das Risikomanagement mit kontextbasierten, geführten Behebungsmaßnahmen, sodass Sicherheitsbeauftragte Probleme und Verstöße einfach an der Quelle beheben und zukünftige Störungen verhindern können. Funktionsumfang:

- **Effektive Untersuchung und Reaktion,** um Sicherheitsbeauftragte bei der Untersuchung von Datensicherheitsvorfällen dabei zu unterstützen, potenzielle Grundursachen schnell zu verstehen.
- **Umfassende geführte Fehlerbehebung,** um funktionsübergreifenden Teams mit automatisierten Arbeitsabläufen und Schritt-für-Schritt-Anleitungen mit vollständigem Kontext zu helfen, Datensicherheitsrisiken anzugehen und wirksam zu beheben.
- **Schnellere Sicherheitsmaßnahmen**: Sicherheitsbeauftragte können userdefinierte Echtzeitwarnungen konfigurieren, um mit schnellen Änderungen an Daten und ihrer Umgebung Schritt zu halten und so Untersuchungen und Reaktionen zu beschleunigen.
- **Nahtlose Integration** für eine einfache Einbindung in vorhandene ITSM-, SIEM- oder ChatOps-Tools und -Plattformen für Warnmeldungen, Fehlerbehebung, Anleitungen und Arbeitsabläufe.

Erleben Sie Zscaler DSPM

Demo anfordern
Sehen Sie Zscaler DSPM in Aktion in einer geführten Demo.

Demo anfordern

Laden Sie den DSPM-Kaufratgeber herunter.
Informieren Sie sich über die fünf wichtigsten Anforderungen, die Sie bei der Auswahl der richtigen DSPM-Lösung für Ihr Unternehmen berücksichtigen sollten.

Jetzt herunterladen

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

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Anhang

Glossar

- Data Security Posture Management (DSPM)
- Cloud Native Application Protection Platform (CNAPP)
- Cloud Security Posture Management (CSPM)
- Cloud Infrastructure Entitlement Management (CIEM)

Weitere Beiträge zum Thema

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

On-Demand-Inhalte

- Keynote: Zenith Live '24, Zscaler DSPM: Sichere Cloud-Daten mit einer komplett integrierten Plattform — Erfahren Sie mehr über die Umstellung auf DSPM bei Inter&Co.
- Webinar: Warum ist DSPM eine unverzichtbare Komponente Ihrer Data Protection-Strategie?

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 Datenverlust. Die SSE-basierte Zero Trust Exchange ist auf über 150 Rechenzentren der ganzen Welt verteilt und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf **zscaler.com/de** oder folgen Sie uns auf Twitter unter **@zscaler**.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ und weitere unter **zscaler.com/de/legal/trademarks** aufgeführte Marken sind entweder (i) eingetragene Marken bzw. Dienstleistungsmarken oder (ii) Marken bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.

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