Zscaler™ Data Protection auf einen Blick

Die Einführung von SaaS und öffentlichen Clouds hat dazu geführt, dass Daten inzwischen weit verteilt sind und sich nur schwer, wenn überhaupt, mit herkömmlichen Schutz-Appliances absichern lassen. Daher ist es sowohl für unvorsichtige User als auch für Angreifer ein Leichtes, Unternehmensdaten aus der Cloud offenzulegen.

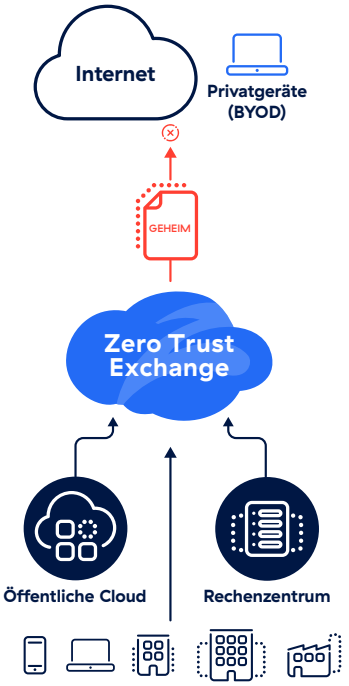
Zscaler Data Protection folgt den Usern und den Anwendungen, auf die sie zugreifen, und schützt sie überall und jederzeit vor Datenverlusten. Unsere Zero Trust Exchange™ überprüft Inline- und Cloud-Daten, um sicherzustellen, dass alle Daten überall sicher sind, und bietet gleichzeitig einen optimierten Ansatz für Schutz und Betriebsabläufe.

Zscaler Data Protection bietet integrierten Schutz vor allen Quellen von Datenverlusten:

Verhinderung von Inline-Datenverlusten im Web und für BYOD

Wenn User auf das Internet und seine riskanten Ziele zugreifen, stellt dies eine Bedrohung für Ihre Unternehmensdaten dar. Legacy-Appliances sind nicht in der Lage, Usern außerhalb des Netzwerks zu folgen oder ihren Web-Traffic zu schützen.

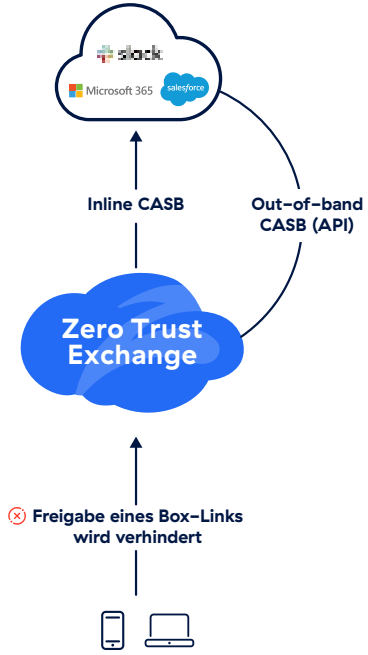
Zscaler ist eine cloudnative Plattform, die skalierbar ist, um den gesamten Traffic überall zu überprüfen. Eine einzige DLP-Richtlinie schützt Daten im Web, in SaaS- und privaten Anwendungen und bietet darüber hinaus erweiterte Klassifizierungen wie EDM, IDM und OCR. Nutzen Sie die Browser-Isolierung, um Daten sicher als Pixel auf nicht verwaltete BYOD-Geräte zu streamen.



Schutz von SaaS-Daten mit CASB

Die Absicherung von ruhenden Daten in SaaS-Anwendungen ist entscheidend für die allgemeine Sicherheit — mit nur zwei Klicks können Sie Daten über Anwendungen wie Microsoft OneDrive mit nicht autorisierten Usern teilen.

Zscaler bietet einen integrierten, multimodalen CASB, mit dem SaaS-Anwendungen abgesichert werden können — und das ohne die Kosten und Komplexität einer Einzellösung. Mithilfe der Inline-Funktionen lässt sich die gesamte Shadow-IT zuverlässig erkennen und kontrollieren. Out-of-band-DLP und ATP-Funktionen unterstützen die Behebung riskanter Dateifreigaben und Erkennung von ruhender Malware in der Cloud.



Schutz von Daten auf Endgeräten

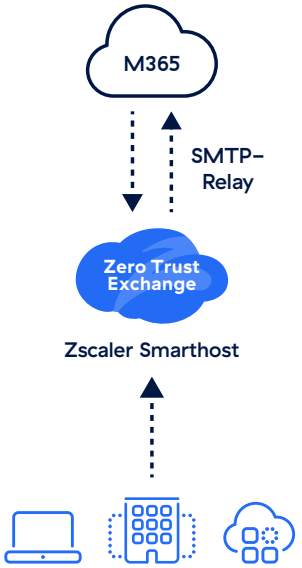
Daten, die auf Endgeräten verwendet werden, können über mehrere Kanäle leicht verloren gehen. Von Wechseldatenträgern über Druckvorgänge bis hin zu Netzwerkfreigaben setzen User sensible Daten oft unnötigen Risiken aus, oder sie exfiltrieren Daten in böswilliger Absicht, wenn sie zu einem anderen Unternehmen wechseln.

Mit Endgeräte-DLP können Unternehmen konsistente DLP-Richtlinien für alle Endgeräte durchsetzen und so sicherstellen, dass sensible Daten geschützt bleiben. Kontrollieren Sie USB-Laufwerke, Bluetooth, Druckvorgänge oder Netzwerkfreigaben mit stets aktivem DLP-Schutz.

E-Mail-DLP über Smarthost

E-Mail ist einer der häufigsten Kanäle für Datenverluste. User können vertrauliche Daten problemlos aus der Organisation heraus oder an private E-Mail-Konten weiterleiten.

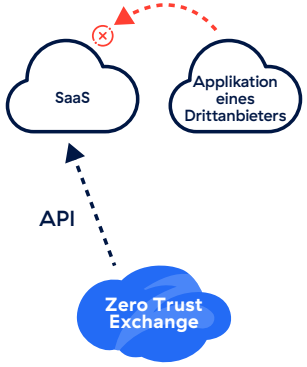
Mit Zscaler Email DLP können Sicherheitsadministratoren auf einfache Weise eine DLP-Überprüfung in ihre E-Mail-Architektur integrieren. Zscaler wird als Smarthost implementiert und kann über SMTP-Relay als nächster Hop nach Ihrem E-Mail-Service hinzugefügt werden. Setzen Sie DLP-Überprüfung und Aktionen wie Blockieren, Verschlüsseln und Quarantäne mit minimalen Änderungen an Ihren E-Mail- oder MTA-Einstellungen durch.



Einheitliche SaaS-Sicherheit (SSPM, SaaS-Lieferkette, CASB)

Viele Datenpannen in der Cloud werden durch gefährliche Fehlkonfigurationen, Zugriffe oder Drittanbieteranwendungen verursacht, die mit SaaS-Plattformen verbunden sind. Das Verständnis und die Kontrolle Ihres SaaS-Sicherheitsstatus ist ein wichtiger Schritt, um die riesigen Mengen an sensiblen Daten in diesen Clouds zu schützen.

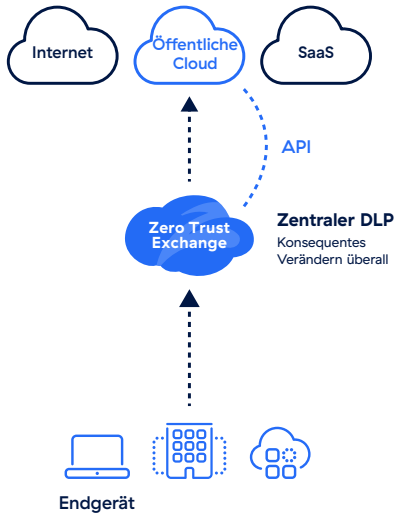
Mit der einheitlichen SaaS-Sicherheit von Zscaler erhalten Unternehmen einen ganzheitlichen Ansatz zum Scannen und Absichern von SaaS-Plattformen wie Office 365 oder Google. Sie erhalten einen detaillierten Einblick in gefährliche Fehlkonfigurationen und Anwendungsintegrationen mit automatischer Behebung, Anleitung und Kontrolle über die Sperrung riskanter verbundener Anwendungen.



Data Security Posture Management (DSPM)

Sensible Daten, die in öffentlichen Clouds wie AWS und Azure gespeichert sind, können sehr dynamisch sein. Von übermäßigen Berechtigungen und Schwachstellen bis hin zu Schattendaten benötigen IT-Teams eine bessere Möglichkeit, Daten in öffentlichen Clouds zu erfassen, zu katalogisieren und abzusichern.

Die DSPM-Lösung von Zscaler erkennt sensible Daten schnell, ermittelt Risiken und kontrolliert Zugriff und Sicherheitsstatus. Das Beste daran ist, dass das integrierte DSPM von Zscaler dieselbe DLP-Engine wie alle anderen Kanäle (Endgerät, Netzwerk, SaaS) nutzt, sodass die Warnmeldungen konsistent sind, unabhängig davon, wohin sich Ihre Daten bewegen.



Zscaler Data Protection — Kernfunktionen

Einheitlicher Schutz mit unbegrenzter SSL-Überprüfung

Zscaler Data Protection bietet konsistente, einheitliche Sicherheit für in Übertragung befindliche und ruhende Daten in SaaS- und öffentlichen Cloud-Anwendungen.

Sicherheit für generative KI-Anwendungen

Schützen Sie Daten vor riskanten generativen KI-Anwendungen mit detaillierten Einblicken in User-Prompts und granularen Richtlinienkontrollen.

KI-gestützte Datenerkennung

Die automatische Erkennung von Zscaler auf Endgeräten, im Netzwerk und in der Cloud verbessert die Datentransparenz und verkürzt die Reaktionszeiten auf Risiken erheblich.

Workflow-Automatisierung und User-Coaching

Eine speziell entwickelte Plattform für das Incident Management bei Datenverlusten mit leistungsstarken Optionen, durch die User Begründungen für Verstöße liefern und Schulungen erhalten können.

Komponenten von Zscaler Data Protection

		Zscaler Essentials Platform	Zscaler Plattform
Data Protection Standard	Stoppen Sie Datenverluste mit Cloud App Control, Shadow IT, Tenancy Restrictions, Inline Web DLP (Monitor Only) und CASB für 1 App.	Inbegriffen	Inbegriffen
Inline Web DLP — Alle Apps	Verhindern Sie Datenverluste mit vollständigem Inline-Web-DLP im Web, in Gen AI und in privaten Unternehmensanwendungen	ADD-ON	Inbegriffen
Email DLP	Echtzeit-Schutz vor Datenverlust für Corporate Exchange Online	ADD-ON	ADD-ON
DLP für Endgeräte	Sichere Datennutzung auf verschiedenen Endgeräten	ADD-ON	ADD-ON
Einheitliche SaaS-Sicherheit (SSPM, CASM, Lieferkette)	Verwalten und kontrollieren Sie SaaS-Daten und -Status auf einer einheitlichen Plattform	ADD-ON	ADD-ON
Erweiterte Datenklassifizierung und -verschlüsselung	Verwenden von EDM, IDM, OCR für Fingerabdrücke von userdefinierten Daten, Formularen und Bildern (Screenshots) Daten können geschwärzt, verschlüsselt und mit Wasserzeichen versehen werden	ADD-ON	ADD-ON
BYOD-Isolierung (erweitert)	Verhindern Sie BYOD und nicht verwaltete Geräte beim Zugriff auf SaaS-Apps (User Portal 2.0).	ADD-ON	ADD-ON
Data Security Posture Management (DSPM)	Schnelles Erkennen, Klassifizieren und Schützen sensibler Daten in der öffentlichen Cloud	ADD-ON	ADD-ON

Weitere Informationen über die Vorteile von Zscaler Data Protection finden Sie unter zscaler.de/dp.

zscaler™ | Experience your world, secured.™

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 SASE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Weitere Informationen finden Sie auf **zscaler.de** oder auf Twitter unter **@zscaler**.

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