E-BOOK

Zuverlässige Datensicherung in einer „Work-From-Anywhere“-Welt

Zscaler Data Protection: Zuverlässiger Schutz für alle geschäftskritischen Daten



© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Inhalt

Größte Herausforderungen	03
Zscaler-Lösung	04
Out-of-Band CASB	05
Inline CASB	06
Endpoint DLP	07
E-Mail DLP	08
KI-gestützte automatische Datenerkennung	09
Erweiterte Klassifizierung	10
Sicherheit für generative KI	11
Einheitliche SaaS-Sicherheit	12
Data Security Posture Management (DSPM)	13
Browser-Isolierung	14
Workflow-Automatisierung	15
Zusammenfassung	16

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Die zuverlässige Sicherung geschäftskritischer Daten ist heute so schwierig wie nie zuvor

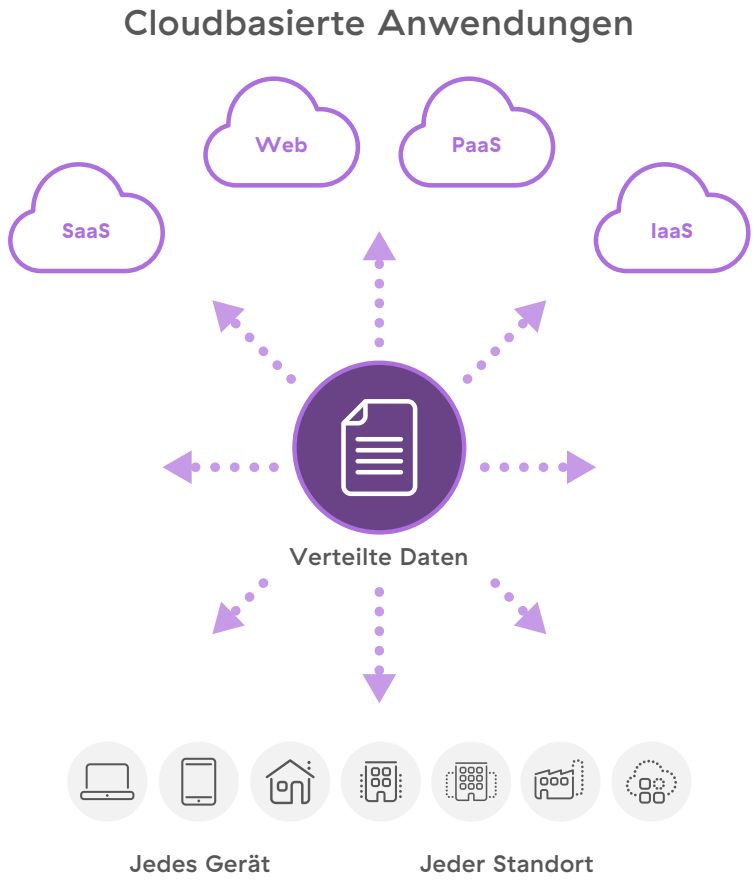
Durch cloudbasierte Anwendungen sind Daten über verschiedene Umgebungen verteilt, und die Mitarbeiter greifen von den unterschiedlichsten Standorten innerhalb und außerhalb des Netzwerks darauf zu. Herkömmliche Lösungen für die Data Protection bieten aus mehreren Gründen keinen adäquaten Schutz mehr:

Mangelnde Kontrolle
Da der Zugriff auf cloudbasierte Anwendungen außerhalb des Netzwerks und der Kontrollmaßnahmen des Unternehmens übers Internet erfolgt, können Daten nicht mehr zuverlässig geschützt werden.

Eingeschränkte TLS/SSL-Überprüfung
Der Traffic ist größtenteils verschlüsselt. Da herkömmliche Ansätze für die Data Protection SSL/TLS-Datenverkehr jedoch nicht in großem Umfang überprüfen können, werden potenzielle Risiken nicht erkannt.

Mangelnde Transparenz
Durch die unübersichtliche Verteilung cloudbasierter Anwendungen über unterschiedliche Standorte und User-Gruppen wird die Überprüfung der Compliance erschwert.

Unübersichtliche Umgebungen
Durch Einzelprodukte und nachträgliche Aufstockungen des Security-Stacks entstehen komplexe Umgebungen, die eine klare Sicht auf die Risiken versperren.



© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Die Lösung von Zscaler

Zscaler gibt Unternehmen die Kontrolle über ihre Daten zurück

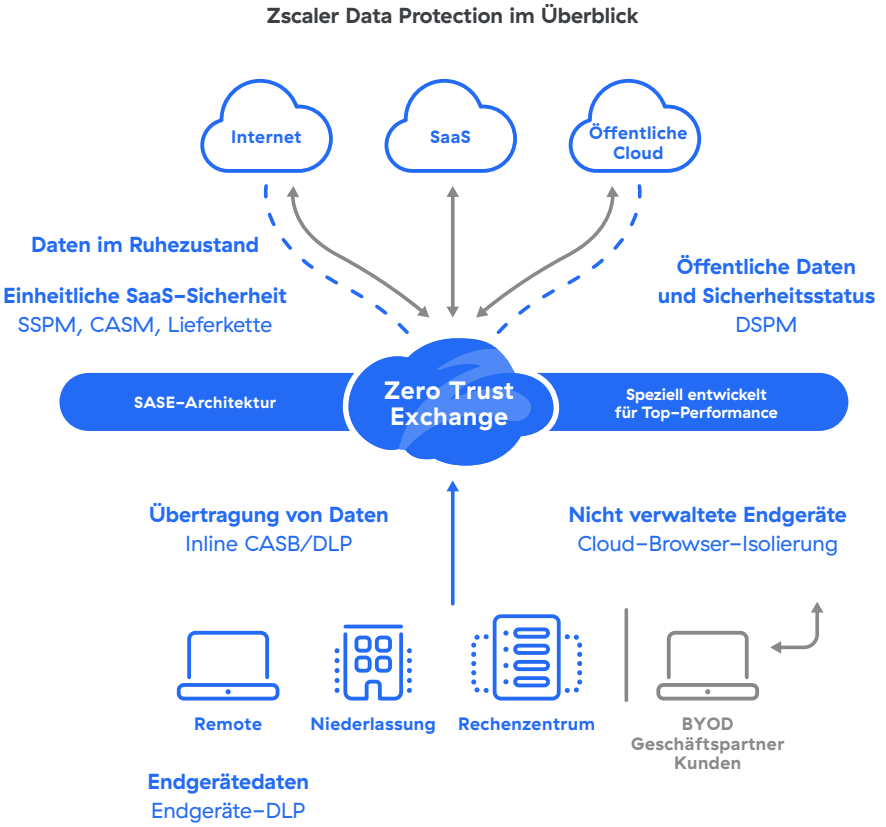
Zscaler Data Protection unterstützt die Gewährleistung einer konkurrenzlos zuverlässigen Data Protection durch konsequente Umsetzung mehrerer Kernprinzipien:

Speziell entwickelte SASE-Architektur
Echtzeitschutz für alle User mithilfe einer hochleistungsfähigen Inline-Cloud, die über 150 Rechenzentren weltweit verteilt ist.

SSL-Überprüfung in großem Maßstab
Überprüfung des gesamten SSl-Traffics auf Exposition von Daten mit unbegrenzter Überprüfungskapazität pro User.

Compliance-Einblicke
Scannen von SaaS-Lösungen, Microsoft 365 und Anwendungen in öffentlichen Clouds auf Verstöße und Fehlkonfigurationen zur zuverlässigen Gewährleistung der Compliance.

Eine Plattform, eine Richtlinie, vollständige Transparenz.
Sichern Sie alle Cloud-Datenkanäle — Daten in Bewegung, im Ruhezustand und auf allen Endgeräten und Cloud-Umgebungen — mit einer einfachen, einheitlichen Plattform.



© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Out-of-band CASB: Zuverlässiger Schutz für zugelassene Anwendungen

Cloudbasierte Anwendungen ermöglichen eine bessere Zusammenarbeit insbesondere angesichts der gestiegenen Anzahl von Remote-Mitarbeitern, erhöhen aber auch das Risiko der Exposition von Daten. Die unwissentliche Fehlnutzung dieser Anwendungen kann sie für schädliche Aktivitäten anfällig machen.

So schützt Zscaler Out-of-Band CASB cloudbasierte Anwendungen und Daten:

- **Schutz für ruhende Daten**
  Geschäftskritische Daten in cloudbasierten Anwendungen, E-Mails und Filesharing-Services werden erkannt und DLP-Richtlinien zur Zugriffskontrolle und Minimierung der Exposition durchgesetzt.

- **Keine riskanten Datenfreigaben.** Setzen Sie detaillierte Richtlinien für vertrauliche Daten im Ruhezustand durch, um sicherzustellen, dass diese nicht außerhalb des Unternehmens weitergegeben werden.



- **Behebung von Bedrohungen** Durch Scannen von Daten-Repositories in File-Hosting-Services wie OneDrive und Box werden schädliche Inhalte schnell erkannt und in Quarantäne verschoben.

- **Vereinfachte Data Protection** Durch eine einheitliche Plattform, die eine einzige Policy zur Datensicherung für sämtliche Daten bei der Übertragung und im Ruhezustand durchsetzt, wird die Komplexität unterschiedlicher Einzelprodukte vermieden.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Inline-CASB zur Gewährleistung von Transparenz und Kontrolle in Echtzeit

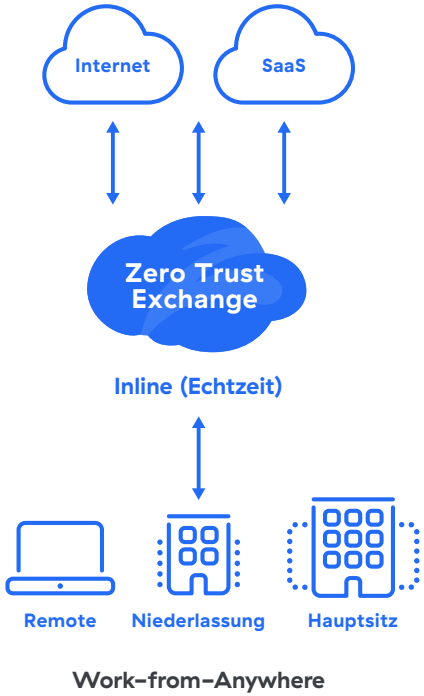
Out-of-Band CASB ermöglicht sowohl die Sicherung von Daten im Ruhezustand als auch Echtzeit-Kontrolle über cloudbasierte Anwendungen. So unterstützt Inline-CASB den sicheren Wechsel in die Cloud:

- **Reduziert das Risiko von Schatten-IT.**
  So können Sie schnell erkennen, welche sicheren bzw. unsicheren Cloud-Apps im gesamten Unternehmen verwendet werden.

Beispiel: Der Zugriff potenziell riskanter Anwendungen (z. B. Online-PDF-Konvertierer oder Filesharing-Websites) auf Unternehmensdaten kann durch Sperren dieser Anwendungen verhindert werden.

- **Erzwingt Nutzung offiziell genehmigter Apps.**
  Beschränken Sie die Useraktivität auf die von der IT und dem Unternehmen genehmigten Cloud-Apps.

Beispiel: Durch Zulassen von OneDrive und Sperren von Box kann die Zusammenarbeit über Microsoft 365 und damit auch die Produktivität verbessert werden.



- **Verhindert Datenverlust durch Dateitypkontrollen.**
  Beschränken Sie die Datenübertragung nach Dateitypen durch bedingtes Blockieren und Warnen.

Beispiel: Das Hoch- und Herunterladen von Word-, Excel- oder PowerPoint-Dateien kann für einzelne User oder Gruppen verhindert werden.

- **Erzwingt Mandantenbeschränkungen.**
  Kontrollieren Sie den Traffic, indem Sie nur bestimmte Instanzen von Cloud-Apps zulassen.

Beispiel: Datenlecks, die durch Zugriff der User auf private Instanzen von Microsoft 365 entstehen, können verhindert werden, indem ausschließlich Zugriff auf Microsoft 365 für Unternehmen zugelassen wird.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Vereinfachte Kontrolle von Gerätedaten mit Endgeräte-DLP

Eine Strategie für Endgeräte ist die Voraussetzung für erfolgreiche Data Protection. Mit Endpoint DLP profitieren Sie von umfassendem Endgeräte-Schutz ohne die Komplexität herkömmlicher Ansätze.

- **Einheitliche Richtlinien und Transparenz**
  Dank einer zentralisierten DLP-Engine erhalten Sie konsistente Warnmeldungen — für Endgeräte, inline und in der Cloud.
- **Ein einziger ressourcenschonender Agent**
  Die Integration in den bestehenden Agent von Zscaler gewährleistet eine bessere User Experience, da weniger Agents auf Ihrem Endgerät erforderlich sind.
- **Schnelle Bereitstellung**
  Um die Implementierung zu beschleunigen, können Sie mit Ihren bereits erstellten Zscaler-DLP-Richtlinien arbeiten.
- **Schnelleres Incident Management**
  Mit Workflow-Automatisierung sowie detaillierten Dashboards und Forensik können Sie schneller auf Vorfälle reagieren.

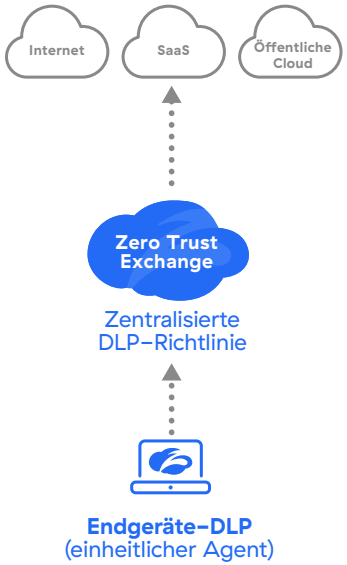
Anwendungsfälle für Endgeräte-DLP

Verbesserte Datenabdeckung:
Stellen Sie sicher, dass wertvolle Daten überall lückenlos erfasst und geschützt werden

Sicherheit bei Kündigungen von Mitarbeitern:
Stellen Sie sicher, dass scheidende Mitarbeiter keine Gerätedaten kopieren und zum neuen Arbeitgeber mitnehmen

Schluss mit veralteter Endpoint DLP:
Ersetzen Sie ein Sammelsurium komplizierter Einzelprodukte durch eine einheitliche Plattform.

Verbesserte Compliance:
Sorgen Sie für die Einhaltung gesetzlicher Vorschriften für alle Dateien und Geräte.



Geschützte Kanäle

Wechseldaten-träger	Synchronisierung des persönlichen Cloud-Speichers
Netzwerkfreigaben	Druck

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Weniger Komplexität mit einem einheitlichen Ansatz für E-Mail-DLP in Echtzeit

Eine der größten Gefahren für Daten geht von E-Mails aus. Mit der E-Mail-DLP von Zscaler erhalten Unternehmen einen leistungsstarken Ansatz für umfassende DLP-Kontrollen von E-Mail-Daten.

Herkömmliche Ansätze zur Absicherung von E-Mail-Daten können umständlich und komplex sein. Mit der Einführung von SSE suchen IT-Teams nach einheitlichen Ansätzen zur Absicherung von Daten in allen E-Mail-Kanälen, die die Komplexität reduzieren.

Mit der E-Mail-DLP von Zscaler, die Smarthost nutzt, lässt sich Data Protection einfach und in Echtzeit auf E-Mails skalieren. Durch die Nutzung von SMTP Relay ermöglicht Zscaler eine mühelose Integration in bestehende E-Mail-Architekturen mit vollständiger Kontrolle über E-Mail-Daten und -Anhänge.

Vorteile der E-Mail-DLP von Zscaler:

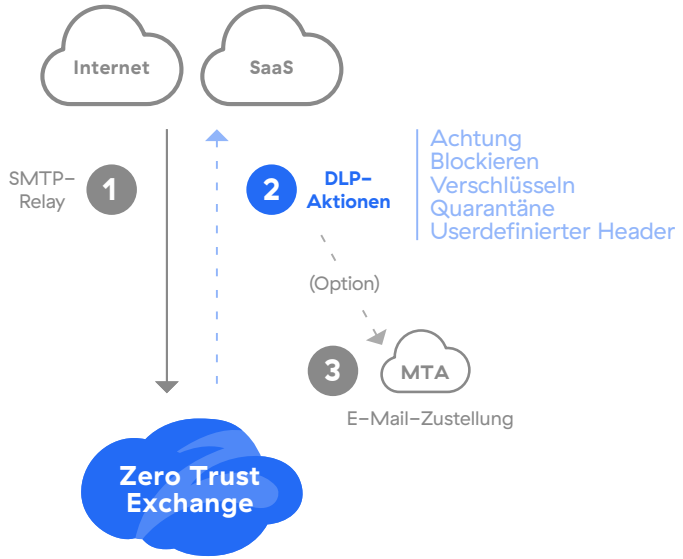
Protokollunabhängig
Kann auf allen verwalteten, nicht verwalteten und sogar auf Mobilgeräten eingesetzt werden

Einfache Bereitstellung
Keine Änderungen des MX-Eintrags erforderlich

Flexible Richtlinien
Anpassbare Richtliniendefinitionen und detaillierte Richtlinienauswertungen

Zentral und einheitlich
Eine einzige Useroberfläche und DLP-Engines für alle Kanäle

E-Mail-DLP in Echtzeit



Zscaler Smarthost

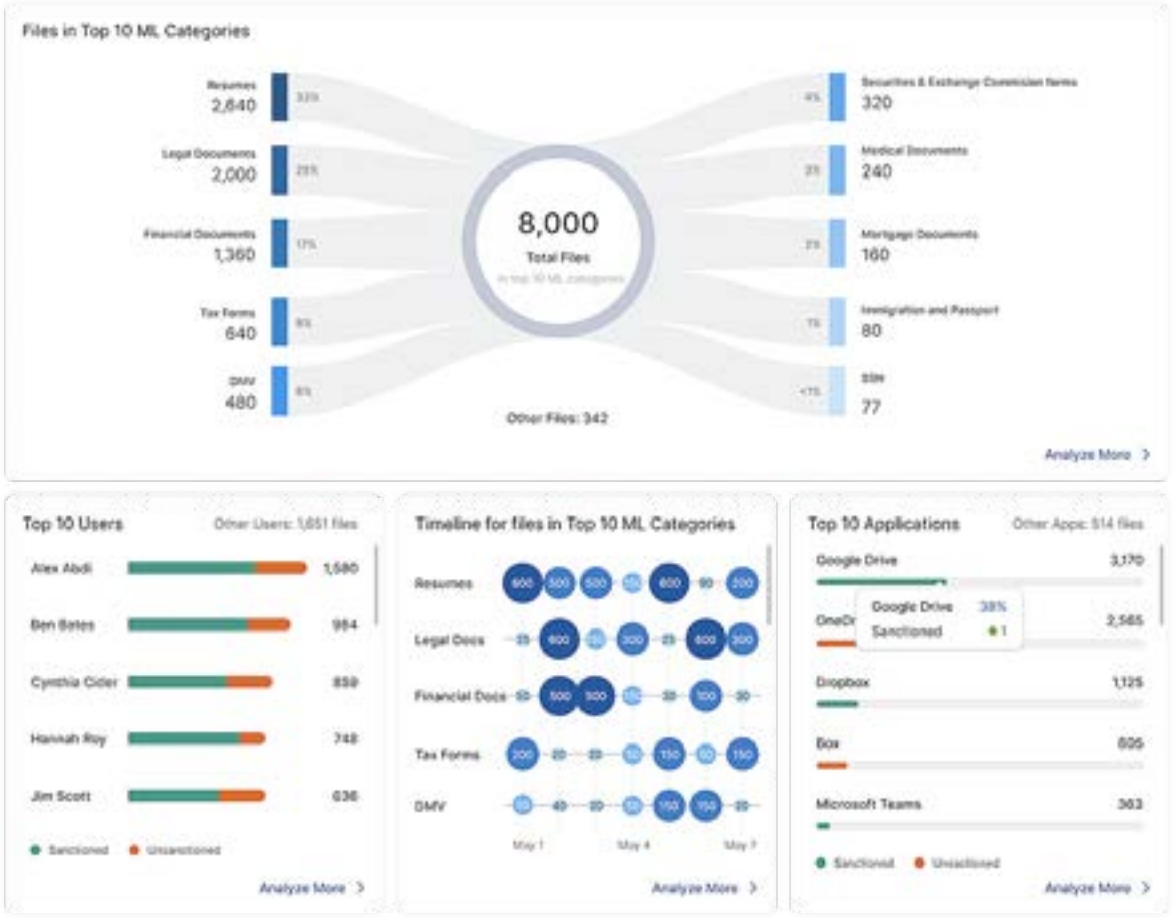
© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Finden und schützen Sie Daten sofort mit KI-gestützter Datenerkennung

Die Implementierung und Inbetriebnahme eines Data Protection-Programms kann manchmal Monate dauern. Mit der innovativen Datenerkennung von Zscaler können Sie das Risiko und die Verhaltensmuster, die mit Ihren Daten verbunden sind, schnell verstehen.

KI-gestützte Datenerkennung:

- Erkennung von Daten auf Endgeräten, Inline und in öffentlichen Clouds
- Schnelles Erfassen von Verlustrisiken durch User und Anwendungen
- Mit wenigen Klicks zur Richtlinienerstellung



© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Klassifizierung und Schutz userdefinierter Daten, Formulare und Bilder

Die Datenklassifizierung ist das Herzstück jedes guten DLP-Programms. Mithilfe erweiterter Datenklassifizierung können Unternehmen bestimmte Kategorien vertaulicher Daten vor Verlusten schützen.

Exact Data Match (EDM)

Fingerabdrücke zum Schutz spezifischer Unternehmensdaten. Beispiel: Auslösung bei Kreditkartennummern von Kunden, nicht bei allen Kreditkartennummern (wie bei einem Amazon-Einkauf)

Indexed Document Match (IDM)

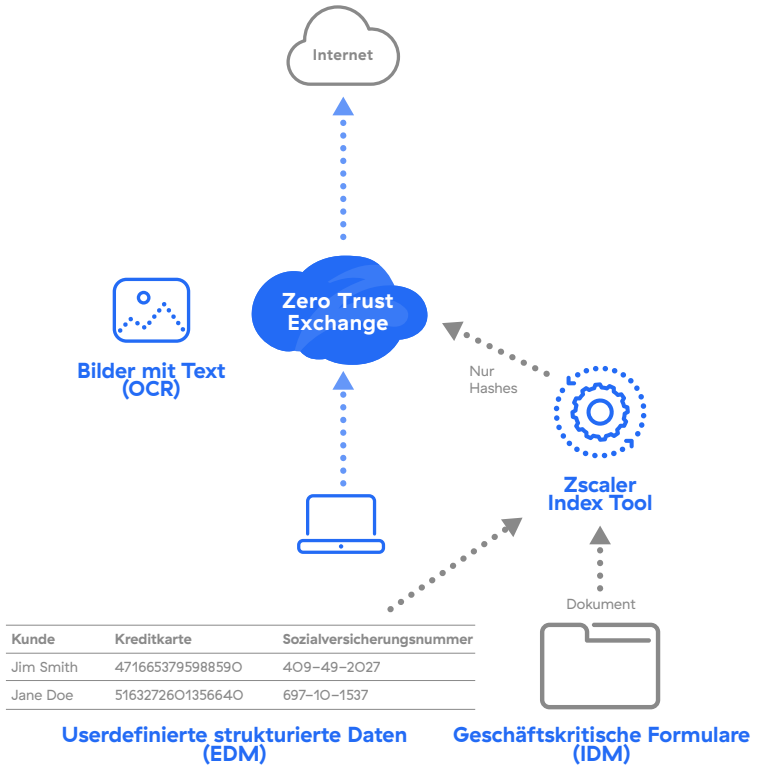
Fingerabdrücke zum Schutz spezifischer Dokumente und Formulare. Beispiel: Erstellen Sie einen Fingerabdruck für ein leeres Steuer- oder Hypothekenformular und sperren Sie alle anderen ausgefüllten Kopien.

Optical Character Recognition (OCR)

Verhinderung von Datenverlusten durch Erkennung von Text in Bildern. Beispiel: Überprüfen Sie Screenshots, die möglicherweise vertrauliche Inhalte enthalten.

Zscaler Indexing Tool

Ergänzendes Fingerabdruck-Tool für EDM und IDM. Erstellt Hashes von EDM- und IDM-Daten und lädt sie zur Richtlinienerstellung in die Zscaler Cloud.



© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Erhalten Sie maximale Transparenz und Kontrolle über generative KI-Anwendungen.

Um das Potenzial von generativer KI zu nutzen, müssen potenzielle Datenverluste durch die betreffenden Anwendungen verhindert werden. Der neue innovative Ansatz von Zscaler vereint alle Schutzmaßnahmen und Informationen an einem Ort.

Generative KI-Apps haben das Potenzial, die Produktivität in Ihrem Unternehmen zu steigern, Sie benötigen jedoch vollständige Transparenz und Kontrolle über diese Apps, um bessere Entscheidungen zur Blockierung treffen zu können.

Mit der innovativen Sicherheitstechnologie von Zscaler für generative KI können IT-Teams alle generativen KI-Anwendungen im gesamten Unternehmen aufspüren und erhalten beispiellose Transparenz, selbst über eingegebene Prompts, sodass sie zuverlässigere Entscheidungen darüber treffen können, was blockiert werden soll.

Geschäftsnutzen

- Einblick in die von den Usern an die KI-Anwendung gesendeten Prompts für vollständige kontextbezogene Transparenz
- Flexible Richtlinienkontrollen für DLP-Überprüfung und Cloud App Controla
- Erzwingen Sie isolierten Zugriff und schützen Sie Daten im Cloud-Browser von Zscaler.

Transparenz über generative KI

Erkennung von Schatten-KI
Vollständiger Anwendungskatalog mit allen gängigen KI-Anwendungen

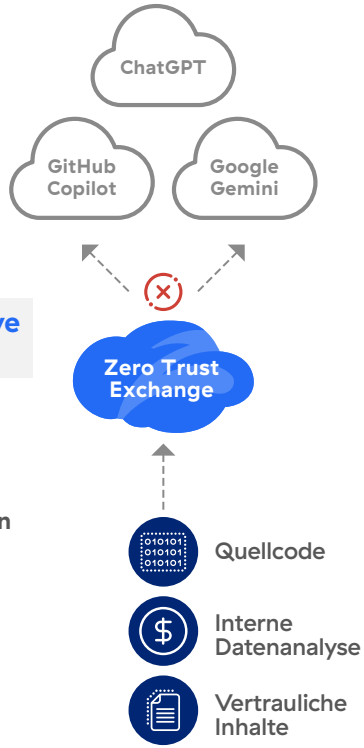
Transparenz über eingegebene Prompts
Sehen Sie die tatsächlichen Prompts, die User an KI-Anwendungen senden

Kontrollmechanismen für generative KI-Anwendungen

DLP-Überprüfung
Blockieren Sie sensible Daten und Inhalte, die an KI-Anwendungen gesendet werden

Kontrolle von cloudbasierten Anwendungen
Kontrollieren Sie den Zugriff auf KI-Anwendungen für alle User, Abteilungen und Standorte

Browser-Isolierung
Beschränken Sie die Nutzung von Daten und Anwendungen auf einen sicheren Cloud-Browser



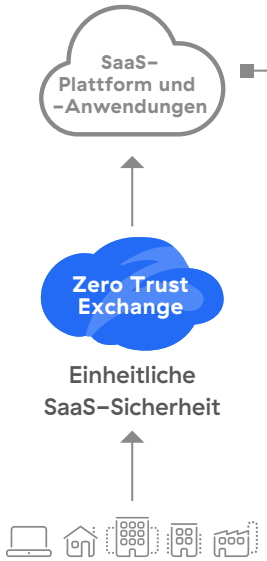
© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Schützen Sie Ihre SaaS-Plattform mit einem vollständig integrierten Ansatz

Zum Absichern von SaaS-Clouds und -Daten sind zu viele Tools erforderlich. Die Kombination von SSPM mit anderen wichtigen SaaS-Sicherheitsansätzen macht es für IT-Teams einfacher, SaaS-Daten und -Sicherheitsstatus zu schützen.

Viele Datenpannen in der Cloud werden durch gefährliche Fehlkonfigurationen 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 SaaS Security Posture Management (SSPM) 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.



Einheitliche SaaS-Sicherheit
Alles zur Absicherung von SaaS an einem Ort

SaaS Security Posture Management (SSPM)
Beheben von Fehlkonfigurationen und Konfigurationsabweichungen

SaaS-Sicherheit für die Lieferkette
Sperren von riskanten Drittanbieter-Integrationen

API-CASB
Verhindern der riskanten Weitergabe vertraulicher Daten

User-Aktivitäten
Überprüfung auf riskante Zugriffe und Mitarbeiter

Verbesserte Kontextdaten, Korrelation und Risikominderung

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Data Security Posture Management (DSPM)

Sichere öffentliche Clouds und Daten mit einem vollständig integrierten Data Protection–Konzept

Data Protection–Teams benötigen einen einheitlichen Ansatz zur Absicherung öffentlicher Cloud–Daten. Zscaler DSPM lässt sich nahtlos in bestehende Data Protection–Programme integrieren.

Vertrauliche Daten, die in öffentlichen Clouds wie AWS und Azure gespeichert sind, können sich sehr dynamisch verhalten. Von übermäßigen Berechtigungen und Schwachstellen bis hin zu Schattendaten benötigen IT–Teams eine bessere Möglichkeit, Daten in öffentlichen Clouds zu erfassen, zu klassifizieren und abzusichern.

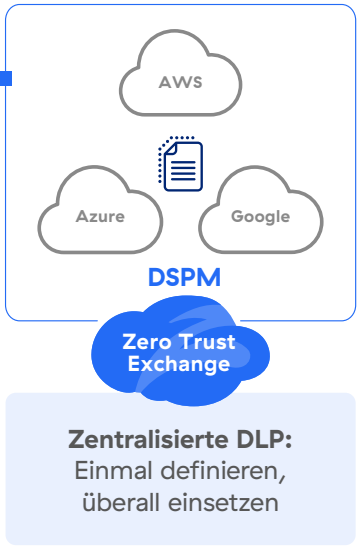
Die DSPM–Lösung von Zscaler erkennt sensible Daten schnell, ermittelt Risiken und kontrolliert Zugriff und Sicherheitsstatus. Das Beste daran ist, dass das integrierte DSPM von Zscaler dieselbe DLP–Engine wie alle anderen Kanäle (Endgerät, Netzwerk, SaaS) nutzt, sodass die Warnmeldungen konsistent sind, unabhängig von der aktuellen Bewegungsrichtung Ihrer Daten.

Geschäftsnutzen

- Schnelles Auffinden sensibler Daten mit KI–gestützter automatischer Erkennung
- Korrelieren von Fehlkonfigurationen, Gefährdungen und Schwachstellen, um das Cloud–Datenrisiko besser nachvollziehen zu können
- Erweitern vorhandener DLP–Wörterbücher auf öffentliche Cloud–Daten für bessere Transparenz und Kontext
- Schnelles Beheben von Risiken mit umsetzbaren Anleitungen zur Problemlösung

Sichere Cloud–Daten und hoher Sicherheitsstatus
Daten finden und schützen und Expositionsrisiken vollständig nachvollziehen

1. **Zuordnung von Datenspeichern**
   Buckets, VMs & DBs mit automatischer Datenerkennung zuordnen
2. **Risikopriorisierung**
   Fehlkonfigurationen und Sicherheitsrisiken für Daten erfassen
3. **Risikobehebung**
   Maßnahmen mit Anleitungen und Richtlinien zur Behebung ergreifen



Zentralisierte DLP:
Einmal definieren, überall einsetzen

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Browser Isolation

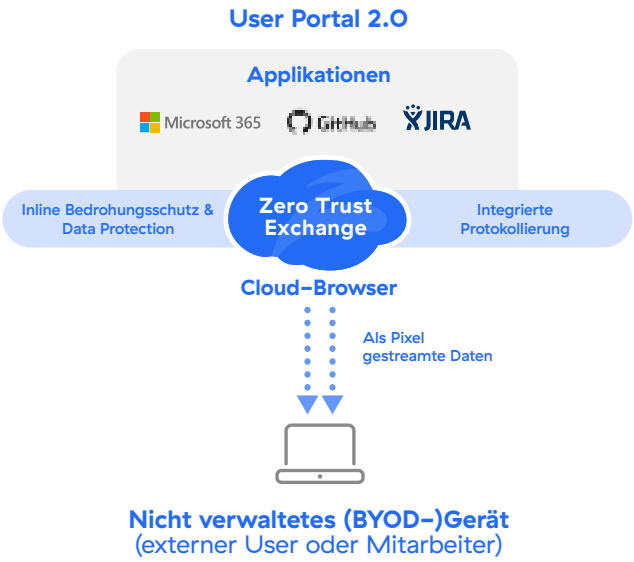
Sichere Webanwendungsdaten und Zugriff für BYOD-Geräte

Partner, Auftragnehmer oder Mitarbeiter benötigen manchmal Zugriff auf Ihre Daten über Privatgeräte. Wie behalten Sie die Kontrolle über Ihre Daten, wenn diese Geräte nicht von Ihnen verwaltet werden?

Mit Zscaler User Portal 2.0 und Browser Isolation können Unternehmen nicht verwaltete Geräte sicher unterstützen. Konkret funktioniert das wie folgt:

So schützt User Portal 2.0 Zugriff und Daten:

- User authentifizieren sich beim Portal und erhalten eine Dashboard-Ansicht der autorisierten Web-Anwendungen (SaaS oder privat). Ein Endgeräte-Agent ist nicht erforderlich.
- User greifen innerhalb eines isolierten Browsers auf die Anwendung zu. Die Daten werden dann sicher in Form von Pixeln auf das Endgerät gestreamt.
- Anwendungen sind vollständig interaktiv, aber das Ausschneiden, Einfügen, Herunterladen und Drucken wird blockiert, und Screenshots werden sogar mit Wasserzeichen versehen.



Vorteile von BYOD:

Bedrohungsschutz und Data Protection
Die gesamte Traffic-Überprüfung erfolgt durch Zscaler inline und gewährleistet so das gleiche Sicherheitsniveau wie bei verwalteten Geräten.

Daten- und Dateiisolierung
Zeigen Sie Dokumente an oder geben Sie Dateien frei (anwendungsübergreifend), ohne die Möglichkeit zum Download oder zur Zwischenablage auf dem Endgerät.

Integrierte DLP-Richtlinien
Nutzen Sie Unternehmensrichtlinien, um einen konsistenten Schutz sensibler Daten und einheitliche Warnmeldungen sicherzustellen.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Besseres Incident Management bei Datenverlusten mit Workflow-Automatisierung

Um Ihr Data Protection-Programm zu optimieren, benötigen Sie ein leistungsfähiges Incident-Management Tool, das Betriebsabläufe rationalisiert und User-Coaching ermöglicht.

Viele Schutzprogramme scheitern an unzusammenhängenden Vorgängen und Tools. Darüber hinaus erfahren die User nie, welche Risiken sie durch den falschen Umgang mit Daten eingegangen sind.

Zscaler Workflow Automation bietet DLP-Administratoren ein spezielles Tool zur Optimierung des Incident Managements.

Da alle forensischen Daten an einem Ort gespeichert sind, können Administratoren riskante Verhaltensweisen schnell erkennen, den Usern Vorfälle zuweisen, damit sie diese begründen können, und schnell Richtlinienmaßnahmen zur Behebung von Vorfällen implementieren.

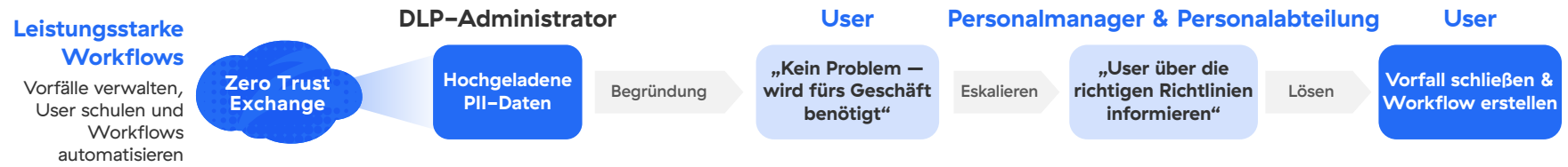
So unterstützt die Workflow-Automatisierung Ihr Data Protection-Programm

Schnelleres Incident Management
Mit einer speziell entwickelten Plattform für das Incident Management bei Datenverlusten sparen Sie wertvolle Zeit.

Automatische Abläufe
Optimieren Sie den täglichen Betrieb durch die Nutzung von Workflows zur Automatisierung sich wiederholender Aufgaben und Eskalationen.

User-Coaching
Erklären Sie Usern über Slack, Teams oder E-Mail Vorfälle und informieren Sie sie gleichzeitig über Best Practices zum Thema Data Protection

Vollständig integriert
Vermeiden Sie häufige Fehler im Schutzprogramm durch die Bereitstellung eines umfassenden Incident-Management-Systems.



© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Maximaler Schutz, minimaler Aufwand

Die Data Protection von Zscaler folgt Ihren Usern und den Anwendungen, auf die sie zugreifen, um Ihre Daten in der Cloud und in Mobil-Umgebungen zu schützen. Die Zscaler Zero Trust Exchange™ ist eine speziell entwickelte Plattform, die den Schutz und die Transparenz bietet, die Sie benötigen, um die Einhaltung von Vorschriften zu vereinfachen und die Data Protection problemlos zu gestalten.

Die Zero Trust Exchange bietet eine Reihe von Vorteilen:

- **Bietet identischen Schutz**, sodass Sie allen Usern unabhängig von ihrer Verbindung oder ihrem Standort eine konsistente Richtlinie für die Data Protection bereitstellen können.
- **Überprüft den gesamten TLS/SSL-Traffic**, um Transparenzlücken zu beseitigen — alles unterstützt durch branchenführende SLAs.
- **Vereinfacht die Einhaltung von Vorschriften**, sodass Sie personenbezogene Daten, medizinische Informationen und Zahlungsdaten problemlos finden und kontrollieren und gleichzeitig die Einhaltung von Compliance-Anforderungen verbessern können.
- **Beseitigt Komplexität** mit einer einheitlichen Plattform, mit der Sie alle Cloud-Datenkanäle sichern können: Daten in Bewegung, im Ruhezustand sowie auf sämtlichen Endgeräten und Clouds.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Zuverlässige Data Protection für eine Cloud- und mobil-orientierte Welt

Ihre Daten befinden sich nicht mehr im Rechenzentrum. Sie befinden sich überall und sind für Mitarbeiter, die außerhalb des Büros arbeiten, praktisch an jedem Ort zugänglich. Ihre bestehenden Sicherheitsansätze können die Daten in einer cloud- und mobil-orientierten Geschäftswelt nicht mehr schützen. Mit Zscaler Data Protection können Sie alle kritischen Daten unabhängig vom Standort der User und der Hosting-Umgebung Ihrer Anwendungen schützen. **Hier erfahren Sie mehr.**

Lesen Sie Kundenberichte zu Zscaler Data Protection >

Zum E-Book

Informationen zur Zscaler Data Protection Platform >

Besuchen Sie unsere Website

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™ sowie weitere unter **zscaler.com/de/legal/trademarks** aufgeführte Marken sind entweder (i) eingetragene Handelsmarken bzw. Dienstleistungsmarken oder (ii) Handelsmarken bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Markenzeichen sind Eigentum ihrer jeweiligen Inhaber.

+1 408 533 0288

Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA

zscaler.com/de