Zukunftsfähige Zero-Trust-Sicherheit für Cloud-Workloads auf AWS.

Herausforderungen

Herkömmliche Netzwerksicherheit ist für Cloud-Workloads ungeeignet

Wenn Unternehmen von physischen On-Premise-Servern auf eine virtualisierte Cloud-Infrastruktur umsteigen, ergeben sich neue Herausforderungen. Herkömmliche Netzwerke und veraltete Sicherheitsmechanismen wie VPNs und Firewalls sind nicht für die Cloud gedacht. Und das bedeutet weniger Sicherheit, geringere Leistung und eine größere Angriffsfläche. Werden Workloads in hybriden Umgebungen bei mehreren Cloud-Anbietern bereitgestellt, wird das Mesh-Netzwerk, das die Workloads miteinander verbindet, zudem immer teurer und schwieriger zu implementieren, zu skalieren und zu verwalten.

Um die digitale Transformation zu beschleunigen, müssen Unternehmen daher alle Workloads, einschließlich ihrer zentralen Anwendungen, effizient in die Cloud verlagern. Denn nur so können sie die Geschäftskontinuität sicherstellen, Effizienzvorteile erzielen und Kosten senken.

Die Zscaler-Lösung

Zero-Trust-Sicherheit mit einfacher Bedienung zum Schutz von Cloud-Workloads

Mit Zscaler Zero Trust Cloud und der branchenführenden Zero-Trust-Architektur können Unternehmen ihre Angriffsfläche verkleinern und die laterale Ausbreitung von Bedrohungen verhindern. Durch Weiterleiten des gesamten ausgehenden Workload-Traffics an die Zscaler Zero Trust Exchange werden konsistente Sicherheitsrichtlinien und Zugriffskontrollen sowie eine vollständige Überprüfung des TLS-/SSL-Traffics durchgeführt. Der Workload-Traffic wird dann direkt an das Ziel weitergeleitet, z. B. an das Internet, SaaS-Anwendungen oder andere Workloads, die in anderen Regionen oder Rechenzentren gehostet werden.

Mit Zscaler entfallen die Kosten und die Komplexität herkömmlicher VPNs und Firewalls. Gleichzeitig profitieren Sie von flexiblem Sicherheits- und Richtlinienmanagement sowie konsistentem Schutz vor Bedrohungen und Datenverlusten.

Geschäftsnutzen

Zscaler Zero Trust Cloud bietet branchenführende[1] Zero-Trust-Sicherheit und einen einfachen, sicheren Internetzugang für Workloads, private Unternehmensanwendungen und öffentliche Clouds

Keine laterale Ausbreitung von Bedrohungen

Die Direct-to-Cloud-Architektur stellt Zugriff mit minimaler Rechtevergabe für Cloud-Workloads und -Anwendungen bereit, verlagert den Traffic aus dem Unternehmensnetzwerk und unterbindet die laterale Ausbreitung von Bedrohungen.

Konsistente Bedrohungsabwehr und einheitliche Data Protection

Verhindern Sie Zero-Day-Angriffe und schützen Sie Daten mit TLS-Überprüfung im Cloud-Maßstab, Segmentierung (zwischen Regionen, öffentlichen Clouds) sowie Schutz vor komplexen Bedrohungen und Datenverlusten.

Geringere Komplexität und Kosten

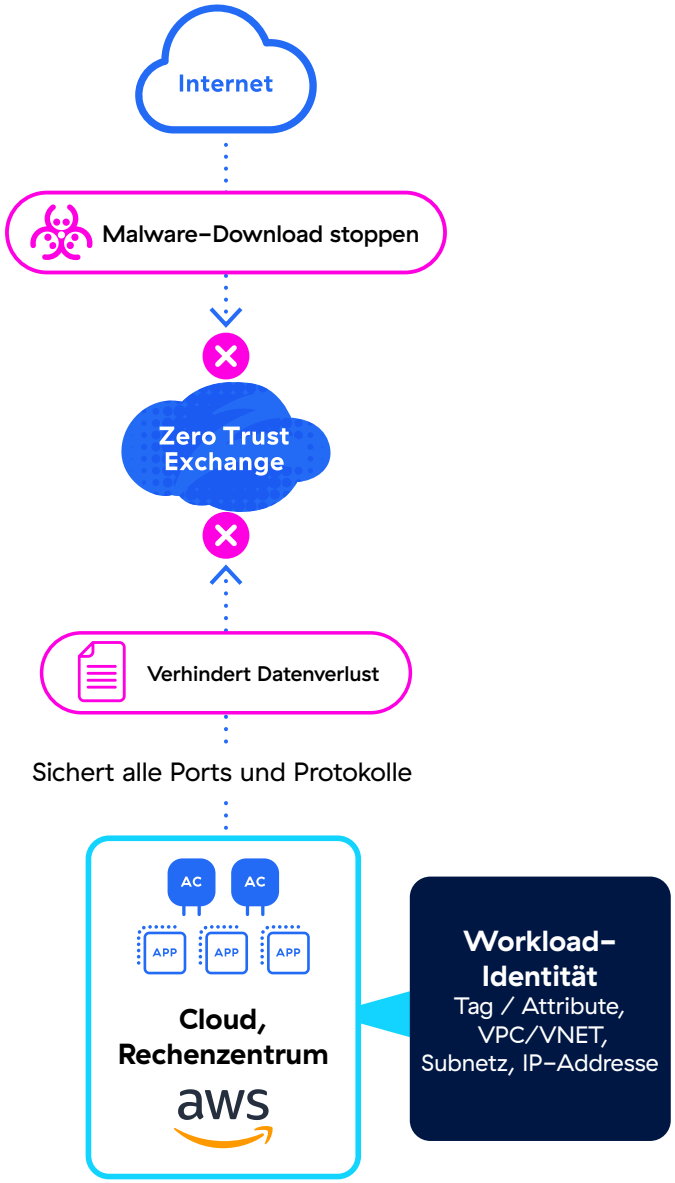
Keine IP-Überschneidungen, Routingverteilung und kostspielige Legacy-Einzelprodukte (VPNs, Firewalls usw.)
Automatisierte Bereitstellung und konsistente Sicherheit für alle Workloads

[1]Gartner: Magic Quadrant for Security Service Edge (SSE), 15. April 2024

Zscaler in AWS

Die Zscaler Zero Trust Exchange ist die weltweit größte Inline-Security-Cloud und schützt Tausende von AWS-Kunden. Zscaler verbindet User sicher mit Workloads sowie Workloads und Geräte untereinander, mit über 160 PoPs weltweit und in vielen AWS-Regionen einschließlich GovCloud East und West. Sie arbeitet im Hyperscale-Modus und kann jede Zunahme des Workload- oder Servertraffics durch flexible horizontale Skalierung bewältigen.

Beispiel: Workload zum Internet



Einheitlicher, umfassender Schutz vor Bedrohungen und Daten durch gemeinsame Sicherheitsrichtlinien für alle Umgebungen

Fallstudie: Micron

Herausforderungen

Sicherung von Usern und Workloads in der hybriden Multicloud durch konsistente Kontrollen, Bekämpfung von Bedrohungen und Schutz geistigen Eigentums

Ergebnisse

- Halbierung der Betriebskosten
- Konsistente Richtlinien für alle User und Workloads reduzieren Risiken
- Sicherer Direktzugriff auf Internet und SaaS-Anwendungen
- Positive User Experience
- Deutlicher Rückgang der Cyberangriffe

„Das Fantastische an Zscaler ist, dass die Lösung alles bietet, was wir von einer Zero-Trust-Plattform erwarten: skalierbare SSL-Trafficprüfung sowie weitere Funktionen zur Bedrohungsprävention und Data Protection."

Nitin Negi
Senior Manager for Cybersecurity Engineering and Operations
Micron Technology

Besuchen Sie uns noch heute im AWS Marketplace und erfahren Sie mehr über Zscaler für AWS und Zero Trust Cloud.

zscaler™ | Experience your world, secured.™

Über Zscaler
Zscaler (NASDAQ: ZS) (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die Zscaler Zero Trust Exchange schützt unzählige Kunden mit standortunabhängig sicheren Verbindungen zwischen Usern, Geräten und Anwendungen vor Cyberangriffen und Datenverlusten. Die in 160 Rechenzentren auf der ganzen Welt verfügbare SASE-basierte Zero Trust Exchange ist die weltweit größte Inline-Cloud-Sicherheitsplattform. Weitere Informationen finden Sie auf **zscaler.com/de**. Folgen Sie **@zscaler** auf X.

©2025 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™, Zscaler Digital Experience™ und ZDX™ sind (i) eingetragene Markenzeichen bzw. Dienstleistungsmarken oder (ii) Markenzeichen bzw. Dienstleistungsmarken von Zscaler, Inc. in den Vereinigten Staaten und/oder anderen Ländern. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.

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