Zscaler™ Workload Communications auf einen Blick

Vorteile:

Keinerlei Angriffsoberfläche

Wenn das Unternehmensnetzwerk keine ausgehende Kommunikation mehr vermittelt, werden die Angriffsfläche des Netzwerks und die laterale Ausbreitung von Bedrohungen eliminiert. So lassen sich Anwendungen vor Kompromittierung schützen.

Schutz vor Datenverlusten

Wenn Workloads nicht mehr über das Unternehmensnetzwerk, sondern direkt kommunizieren, können Workload-Daten nicht mehr abgefangen werden und Cyberkriminelle können sich nicht mehr lateral bewegen, um auf unternehmenskritische Daten zuzugreifen.

Vereinfachte Cloud-Konnektivität

Komplexität und Herausforderungen von Legacy-Netzwerken können mithilfe einer Zero-Trust-Architektur vermieden werden, die die Workload-Sicherheit und -Kommunikation vom Netzwerk loslöst – in jeder Cloud und jedem Rechenzentrum.

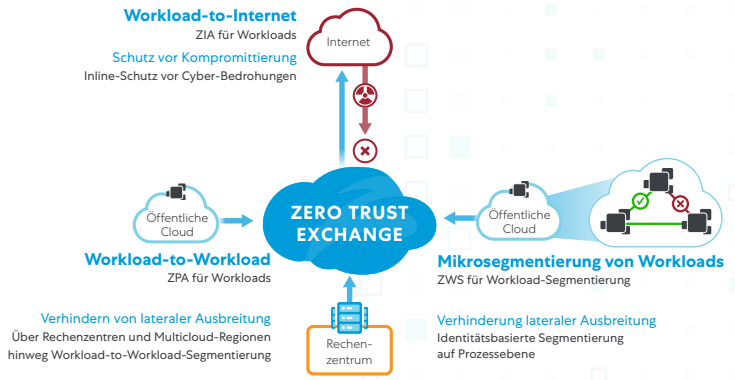
Herausragende Anwendungsleistung

Mit Zscaler Zero Trust Exchange lassen sich Latenzen minimieren und Leistungsengpässe beseitigen. Die Plattform verfügt weltweit über mehr als 150 Präsenzpunkte (Points of Presence, POPs) und ist auf Größe ausgerichtet.

Überblick

Viele Unternehmen migrieren mittlerweile Workloads in die Cloud. Durch die COVID-19-Pandemie wurde es noch deutlicher: Für Unternehmen ist es von großer Bedeutung, die digitale Transformation zu beschleunigen und Strategien für die Migration aller Workloads, einschließlich kritischer Anwendungen, in die Cloud zu entwickeln. So wird Business Continuity gewährleistet, die Widerstandsfähigkeit erhöht, Kosten werden gespart und die Effizienz wird gesteigert. Die Infrastruktur moderner Rechenzentren hat sich von physischen On-Premise-Servern zur Virtualisierung entwickelt, die Anwendungen und Workloads in mehreren Cloud-Umgebungen unterstützt. Die Sicherstellung einer effektiven Workload-Kommunikation in Hybrid- und Multicloud-Umgebungen ist zur Grundlage für den Übergang in die Cloud geworden. Die meisten Unternehmen verlassen sich jedoch nach wie vor auf herkömmliche IP- und Firewall-zentrierte Lösungen, um ihr Netzwerk zu erweitern, und wenden perimeterbasierte Sicherheit an, um ihre Cloud-Strategie umzusetzen. Diese Herangehensweise war zwar angemessen, als sich Anwendungen noch im Rechenzentrum befanden, führt aber in einer Cloud-First-Welt zu Herausforderungen in den Bereichen Sicherheit, Netzwerk und Anwendungsleistung. Angesichts des sich immer mehr beschleunigenden Umstiegs von Unternehmen in die Cloud und der Bereitstellung von Workloads in mehreren Regionen über mehrere Cloud-Anbieter hinweg, wird zudem das Mesh-Netzwerk, das zur Verbindung aller Workloads Verwendung findet, immer kostspieliger sowie schwieriger zu implementieren, zu skalieren und zu verwalten.

Mit Workload Communications hat Zscaler Cloud-Konnektivität komplett neu erfunden: Zero Trust für Cloud-Workloads stellt einfachen, sicheren Workload-Zugriff auf das Internet und private Anwendungen bereit. Im Gegensatz zu Legacy-Netzwerklösungen bietet Workload Communications eine Direct-to-Cloud-Architektur, welche die bewährte Zero-Trust-Exchange-Plattform nutzt, um Vertrauen auf Grundlage von Identität und Kontext zu verifizieren. So wird sichere Workload-to-Internet-Kommunikation, cloudübergreifende Workload-to-Workload-Kommunikation (in sowohl öffentlichen als auch privaten Clouds) und Workload-to-Workload-Kommunikation innerhalb einer Umgebung ermöglicht. Workload Communications bietet eine netzwerkunabhängige Zero-Trust-Fabric, die über das Internet funktioniert, sowie DirectConnect und ExpressRoute, um die Cybersicherheit zu erhöhen, Datenverluste zu verhindern, die Cloud-Konnektivität zu vereinfachen und optimierte Anwendungsleistung im großen Maßstab zu bieten.



Workload Communications – Wichtige Funktionen

Kosteneffiziente Cloud-Konnektivität

VPN-/MPLS-Verbindungen zwischen Clouds und On-Premise-Umgebungen müssen nicht länger bereitgestellt und verwaltet werden. Stattdessen wird der Aufbau von Inside-Out-DTLS-Verbindungen über Multi- und Hybrid-Cloud-Umgebungen über Zscaler Zero Trust Exchange vermittelt.

Sichere Austrittskontrollen

Workload Communications wendet einen Whitelisting-Ansatz mit differenzierten Ausgangskontrollen basierend auf Identität und Standort für Cloud-Anwendungen an, die mit Internet-Services kommunizieren.Darüber hinaus gewährleistet die zentrale Policy-Verwaltung die Durchsetzung konsistenter, standardisierter Sicherheitsrichtlinien in allen Cloud-Umgebungen.

Vollständige Transparenz und Reporting

Workload Communications gewährleistet eine differenzierte, revisionssichere Protokollierung des gesamten weitergeleiteten Anwendungstraffics und der zugehörigen Zugangsinformationen. Außerdem können durch Unterstützung von Nanolog Streaming Service (NSS) alle Protokolle automatisch in Echtzeit zum SIEM des Kunden gestreamt werden.

Bestandteil der weltgrößten Security Cloud

Workload Communications profitiert von der bewährten Größe, Performance und Zuverlässigkeit von Zero Trust Exchange zur Gewährleistung eines sicheren, kontrollierten Zugriffs von beliebigen Clouds ohne exponierte Angriffsfläche.

Differenzierte Zugangskontrollen

Workload Communications stellt identitätsbasierte Anwendungsrichtlinien für die Kontrolle des Zugriffs zwischen Anwendungen, Cloud-Services und Workloads bereit. Die Zugriffskontrolle wird anhand von Standort- und DNS-Attributen unabhängig von Netzwerkinformationen geregelt. Die in Workload Communications konfigurierten Policys unterstützen die flexible Steuerung des Traffics bei Weiterleitung in andere Clouds und ins Internet.

Reibungslose Bereitstellung

Zscaler Workload Communications ermöglicht Zero Touch Deployment und automatische Policy-Konfiguration durch tiefe Integration mit Cloud-nativen Services und Automatisierungstools. Die cloudübergreifende Bereitstellung ist automatisch in wenigen Minuten erledigt.

Weitere Informationen über die Vorteile von Zscaler Digital Experience finden Sie unter **zscaler.de/cloudconnectivity.**

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134, USA
+1 408 533 0288
www.zscaler.de