E-BOOK

Konsistente Sicherheit für Workloads in Multi-Cloud-Umgebungen

Inhalt

Einführung

Unternehmen verlagern Anwendungen und Workloads in beispiellosem Tempo in öffentliche Cloud-Umgebungen — und zwar aus guten Gründen.

Die Cloud-Transformation bringt zahlreiche Vorteile mit sich, die von Kosteneinsparungen bis hin zu verbesserter Betriebseffizienz und mehr reichen. Die Migration in die Cloud ist ein entscheidender Bestandteil der digitalen Transformation. Sie ermöglicht dem Unternehmen, flexibler zu werden, die Anforderungen von Kunden, Anbietern, Lieferanten und externen Partnern besser zu erfüllen und die Kundenerfahrung zu verbessern.

Da immer mehr Unternehmen branchenübergreifend Cloud-Strategien verfolgen, um im Wettbewerb bestehen zu können, ist die öffentliche Cloud zum neuen Rechenzentrum der Unternehmen geworden. Gleichzeitig haben sich Hybrid- und Multicloud-Umgebungen als Norm etabliert. Laut neuen Prognosen von IDC Research wird bis Ende 2025 die Mehrheit der Unternehmen die öffentliche Cloud für generative KI-Plattformen, Entwicklertools und Infrastruktur nutzen, wobei die Cloud-Nutzung die von On-Premise-Systemen übertreffen wird.[1]

Auf die drei größten Cloud-Anbieter entfällt ein Marktanteil von 67 %

31 % aws

25 % Microsoft Azure

11 % Google Cloud

Gartner prognostiziert, dass bis 2025 51 % der IT-Ausgaben für Anwendungssoftware, Infrastruktur und Unternehmensprozessdienste in die öffentliche Cloud verlagert und damit die Ausgaben für traditionelle IT überholen werden.[4]

Trotz der enormen Dynamik der Cloud-Transformation und Prognosen, denen zufolge die Umsätze der Public-Cloud-Anbieter bis Ende 2024 über 800 Milliarden USD erreichen werden,[2] wird der Markt von nur drei Akteuren dominiert:[3]

- Amazon Web Services (AWS) mit einem Marktanteil von 31 %
- Microsoft Azure mit einem Marktanteil von 25 %
- Google Cloud mit einem Marktanteil von 11 %

Diese öffentlichen Cloud-Anbieter bieten ihren Kunden neue Möglichkeiten für mehr Geschwindigkeit, Agilität und Elastizität bei der Nutzung ihrer Rechenressourcen. Sie alle ermöglichen es Entwicklern, in Sekundenschnelle neue Umgebungen zu erstellen. Und alle bieten Hunderte verschiedener Services an — teils mit Selbstverwaltung, teils mit Verwaltung durch den Anbieter.

Diese Faktoren tragen jedoch auch zur Entstehung neuer Sicherheitsrisiken bei, insbesondere für Unternehmen, die zum Schutz ihrer modernen Cloud-Umgebungen weiterhin auf Legacy-Sicherheitsarchitekturen setzen. Die grundsätzliche Diskrepanz zwischen herkömmlichen Ansätzen zur Sicherung lokaler Workloads und den Anforderungen zukunftsfähiger Cloud-Umgebungen macht den Schutz von Cloud-Workloads häufig kostspielig, komplex und schwierig.

1. IDC Research, IDC FutureScape: Worldwide Cloud 2024 Predictions, 2023.
2. IDC Research, Worldwide Semiannual Public Cloud Services Tracker.
3. Statista, Cloud Infrastructure Market, 2024.
4. Gartner, Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025.

Herausforderungen beim Sichern von Cloud-Workloads

Für Unternehmen, die Workloads in die Cloud migrieren, ohne gleichzeitig ihren Sicherheitsansatz zu modernisieren, ergibt sich eine Reihe von Herausforderungen und Risiken.

Eine inkonsistente oder ineffektive Richtliniendurchsetzung setzt Workloads Cyberbedrohungen und -angriffen aus.

Der Versuch, die Sicherheit und Konnektivität von Cloud-Workloads mit Legacy-Ansätzen zu bewältigen, ist zwangsläufig komplex und kostspielig. Auf Firewalls und virtuellen privaten Netzwerken (VPNs) basierende Cybersicherheitsarchitekturen wurden einfach nicht für die heutigen Cloud-Computing-Ökosysteme entwickelt.

Exponierte Workloads können leicht kompromittiert werden. Cyberkriminelle können Unternehmen mit verheerenden Ransomware-Angriffen schädigen. Die Wiederherstellung kann kosten- und zeitaufwendig sein.

Cloud-Workloads erfordern eine umfangreiche Kommunikation mit anderen Workloads und dem Internet. Herkömmliche Sicherheitsansätze sind für diese ständige Konnektivität nicht geeignet.

44 %

waren 2024 von einer cloudbasierten Datenschutzverletzung betroffen.[5]

49 %

berichten, dass die Komplexität der Cloud eine erhebliche Herausforderung für Compliance und Sicherheit darstellt.[6]

69%

erlebten im Jahr 2023 Budgetüberschreitungen bei ihren Cloud-Ausgaben.[7]

5. Thales Group, 2024 Cloud Security Study.
6. Ebenda.
7. Gartner, 2024 Cloud Spending: IT Balances Costs with GenAI Innovation.

Anwendungen in dynamischen Umgebungen erforden dynamischen Zero-Trust-Schutz.

Da Remote- und Hybridarbeit sich als neue Normalität etabliert hat, setzen Unternehmen branchenübergreifend auf Zero Trust, um die Sicherheit ihrer User zu gewährleisten. Bei einem Zero-Trust-Ansatz wird Vertrauen niemals implizit gewährt. Stattdessen wird davon ausgegangen, dass jede Zugriffsanforderung riskant oder kompromittiert ist, und die Anwendungszugriffsanforderung wird nur dann gewährt, wenn folgende Voraussetzungen erfüllt sind:

- Die Identität und der Kontext (das „Wer, Was und Wo“ der Anfrage) können überprüft werden
- Die mit dieser Anfrage verbundenen Risiken können umfassend bewertet werden
- Richtlinien können für jede Sitzung einzeln durchgesetzt werden

Angesichts der zunehmenden Zahl von Anwendungen und Workloads, die in die Cloud verlagert werden, ist es für Unternehmen unerlässlich, beim Anwendungszugriff auf alle Cloud-Ressourcen und -Services das gleiche Schutzniveau zu gewährleisten, das für ihre User gilt. Dies bedeutet, dass Sie die auf Zero Trust basierende Sicherheit auf jede einzelne Ihrer Cloud-Workloads ausweiten.

Wenn Unternehmen ihre älteren monolithischen Anwendungen in die Cloud migrieren, entscheiden sie sich häufig für ein Refactoring mithilfe eines Microservices-Ansatzes. Dadurch können einzigartige Cloud-Funktionalitäten wie spezialisierte Cloud-Datenbanken, serverlose Funktionen und ereignisgesteuerte Architekturen genutzt werden. Dies gewährleistet mehr Effizienz und kann Kosten senken, schafft aber auch eine dynamische, hochautomatisierte Umgebung. In dieser Umgebung findet ein ständiger Kommunikationsaustausch zwischen Workloads statt.

Cloud-Workloads müssen häufig:

- Mit dem Internet kommunizieren
- Mit anderen Workloads kommunizieren

Die schiere Anzahl der zwischen den Workloads zu sendenden Nachrichten ist in dieser Art von Umgebung viel höher als im herkömmlichen Rechenzentrum.

Was ist eine Workload?

Workloads sind die Bausteine heutiger Cloud-Anwendungen. In älteren lokalen Umgebungen waren die meisten Workloads Komponenten innerhalb großer monolithischer Anwendungen. Dies ist in den heutigen Cloud-nativen Umgebungen nicht der Fall, in denen Anwendungen normalerweise aus vielen modularen Komponenten oder Mikrodiensten bestehen. Jeder Service führt eine bestimmte Aufgabe aus und muss zur Ausführug der Unternehmenslogik mit anderen Diensten kommunizieren.

Beispiele für Workloads:

- Container
- Virtuelle Maschinen (VMs)
- VDI-Farmen (Virtuelle Desktop-Infrastruktur)
- Serverlose Funktionen

Herkömmliche Netzwerksicherheit funktioniert nicht für Cloud-native Unternehmen

Viel zu viele Unternehmen haben die Transformation in die Cloud begonnen, ohne ihre Sicherheitsstrategie entsprechend anzupassen. Allerdings wurden herkömmliche Netzwerksicherheitsarchitekturen für das Rechenzentrum vor Ort und nicht für die Cloud entwickelt. Wenn Unternehmen versuchen, sie auf die Cloud zu übertragen, ist die resultierende Architektur hochgradig komplex und ineffektiv.

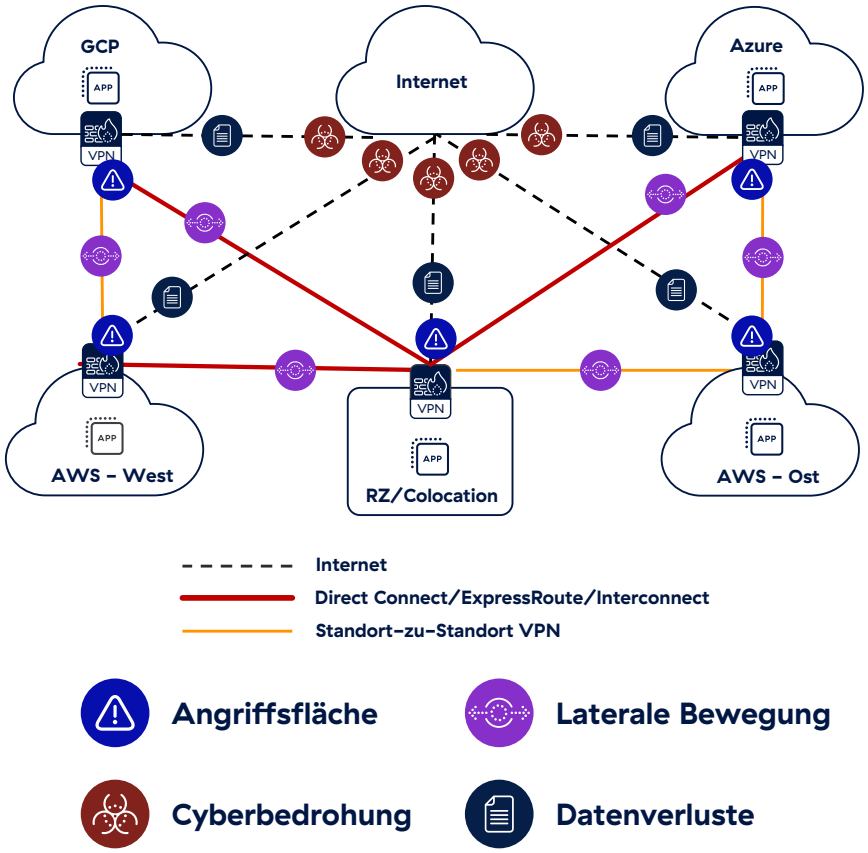
Cloud-Workloads müssen sicher untereinander und mit dem Internet kommunizieren. Der herkömmliche Ansatz zur Erreichung dieses Ziels besteht darin, routingfähige Netzwerke zwischen Cloud-Infrastrukturen mithilfe von Firewalls und VPNs aufzubauen und so das Wide Area Network (WAN) der Unternehmen im Wesentlichen in die Cloud zu erweitern.

In diesem Modell müssen Unternehmen überall dort, wo sich ihre Workloads befinden, virtuelle Firewalls der nächsten Generation (vNGFWs) einrichten. In einer Geschäftswelt, in der Hybrid- und Multicloud-Umgebungen allgegenwärtig sind, entstehen dadurch vollständig vermaschte Netzwerke, in denen jeder Knoten direkt mit allen anderen verbunden ist.
Diese Architektur ist enorm komplex und schwierig zu verwalten.

Wenn Unternehmen zusätzliche Sicherheitsfunktionen implementieren möchten, wie etwa Data Loss Prevention (DLP) oder TLS/SSL-Überprüfung, müssen sie zusätzliche virtuelle Sicherheitsgeräte aufsetzen, was die Komplexität noch weiter erhöht.

Sogar innerhalb der Umgebung eines einzelnen Cloud-Service-Providers müssen Unternehmen mehrere zusätzliche vNGFWs einrichten und verwalten, um den externen und internen Traffic zwischen Cloud-Workloads zu sichern.

Die Workload-Kommunikation vervielfacht die Komplexität und die Sicherheitsherausforderungen



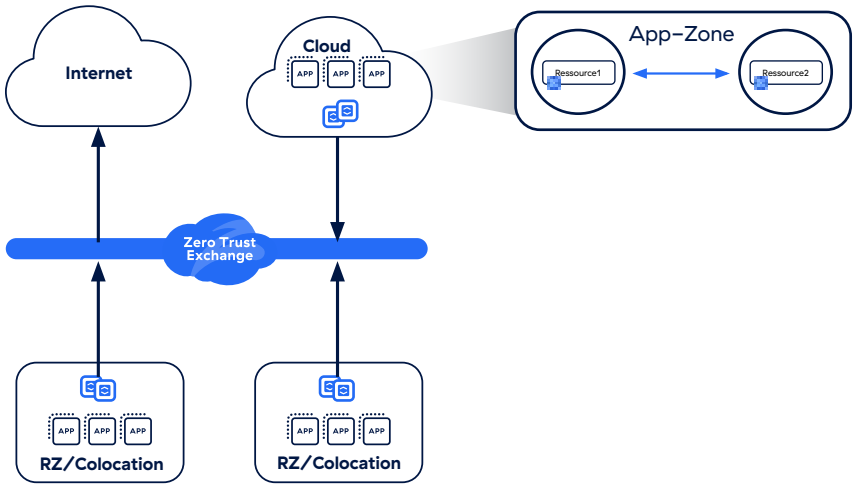
Unzureichende Cyberabwehr für heutige digitale Ökosysteme

Der Versuch, Legacy-Ansätze zur Sicherung und Verbindung von Cloud-Workloads einzusetzen, führt zu einer Reihe von Risiken:

- **Erweiterte Angriffsfläche.** Jede vNGFW hat einen identifizierbaren Netzwerkstandort und kann daher von Angreifern entdeckt werden. Je mehr Firewalls eingesetzt werden, desto größer ist die Angriffsfläche.
- **Kompromittierung der Workloads.** Sobald böswillige Akteure einen Einstiegspunkt in die Umgebung entdecken und sich dort einnisten, können sie die Workload kompromittieren.
- **Laterale Ausbreitung von Bedrohungen.** Da alle Workloads über ein Mesh-Netzwerk verbunden sind, können sich Angreifer, sobald eine einzelne Workload kompromittiert ist, lateral durch das Netzwerk bewegen, um andere zu kompromittieren.
- **Kein Schutz für vertrauliche Daten.** Angreifer können beim Durchqueren des Netzwerks vertrauliche Daten wie Finanzinformationen von Kunden und Geschäftsgeheimnisse finden und exfiltrieren.

Ein neuer Ansatz zur Sicherung von Cloud-Workloads

Die Sicherung der heutigen Enterprise-Computing-Ökosysteme, die stark auf Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) und Software-as-a-Service (SaaS) zahlreicher Cloud-Serviceprovider und -Anbieter basieren, erfordert einen anderen Ansatz, der die Sicherheitsrichtlinien des Unternehmens in den Mittelpunkt seines Netzwerkdesigns stellt. Dies bedeutet, dass ein sicherer Zugriff nach dem Prinzip der minimalen Rechtevergabe basierend auf Direktverbindungen zwischen den Workloads und zwischen den Workloads und dem Internet ermöglicht werden muss. Ein solcher Ansatz vereinfacht auch den Aufbau und die Wartung einer Zero-Trust-Architektur für alle Cloud-Workloads.



Dieser Ansatz bietet eine Reihe von Vorteilen:

- **Die Angriffsfläche wird eliminiert.** Anders als bei herkömmlichen Lösungen sind Workloads für Bedrohungsakteure praktisch unsichtbar, wodurch die gesamte Angriffsfläche im Wesentlichen eliminiert wird.
- **Workloads sind gesichert.** Die vollständige Inline-Inhaltsprüfung zusammen mit DLP-Funktionen bietet robuste Sicherheit für Daten und Workloads.
- **Eine laterale Ausbreitung von Bedrohungen wird verhindert.** Die Bereitstellung einer direkten Konnektivität ohne Verbindung zu einem Netzwerk macht eine laterale Ausbreitung unmöglich.
- **Daten werden geschützt.** Durch die Kombination aus TLS/SSL-Überprüfung in großem Maßstab und DLP-Funktionen ist es möglich, umfassende Data Protection im großen Maßstab bereitzustellen.
- **Komplexität und Kosten werden reduziert.** Durch die Zentralisierung der Cloud-Konfigurationsverwaltung zusammen mit der Sicherheit und die Ermöglichung direkter Konnektivität können Komplexität und Kosten reduziert werden.

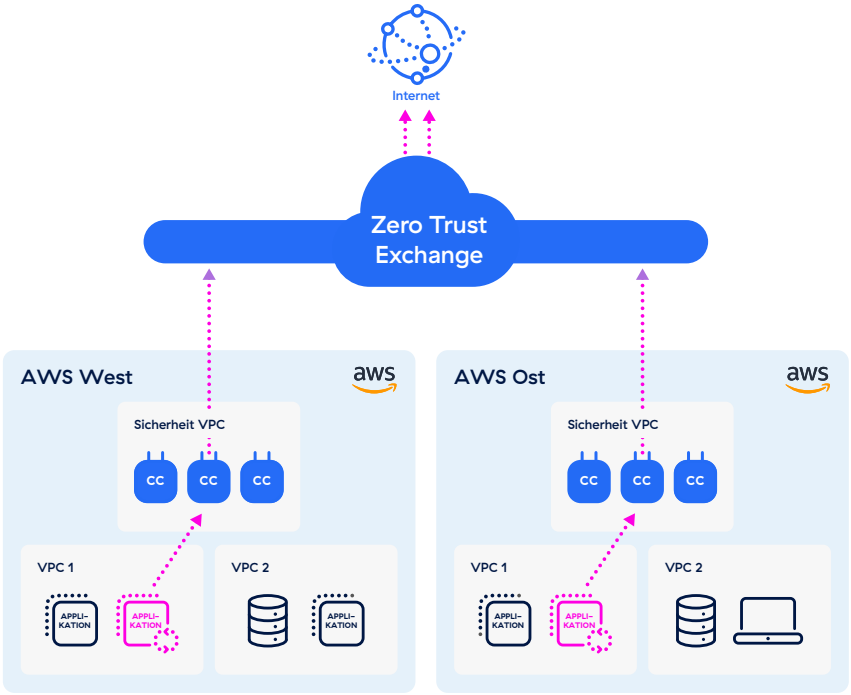
Kommunikation zwischen Workloads und Internet vereinfachen und schützen

Da jede Cloud-Workload auf eine nahezu ständige Kommunikation über das öffentliche Internet angewiesen ist, muss eine Zero-Trust-Lösung für Cloud-Workloads in der Lage sein, alle ausgehenden Verbindungen abzusichern. Innerhalb einer einfachen Direct-to-Cloud-Architektur muss die Lösung einen sicheren Internetzugang für alle Workloads bereitstellen, unabhängig davon, ob sie sich in einer öffentlichen Cloud oder im Rechenzentrum des Unternehmens befinden.

Zu den wichtigsten Funktionen, die zur Sicherung der Workload-Internet-Kommunikation erforderlich sind, gehören:

- Vollständig proxybasierte TLS/SSL-Überprüfung
- Keinerlei Angriffsoberfläche
- Beschränkung des Zugriffs ausschließlich auf genehmigte Websites
- Erweiterter Malware-Schutz zum Blockieren von Zero-Day-Bedrohungen

Stellen wir uns beispielsweise vor, dass Ihr Unternehmen über Apps in AWS West und AWS East verfügt und beide ein Update erfordern. Die Anfrage muss an eine zentrale Plattform weitergeleitet werden, auf der Richtlinien durchgesetzt und verwaltet werden. Eine ideale Lösung kann Zero-Trust-Richtlinien durchsetzen und sichere Verbindungen herstellen.



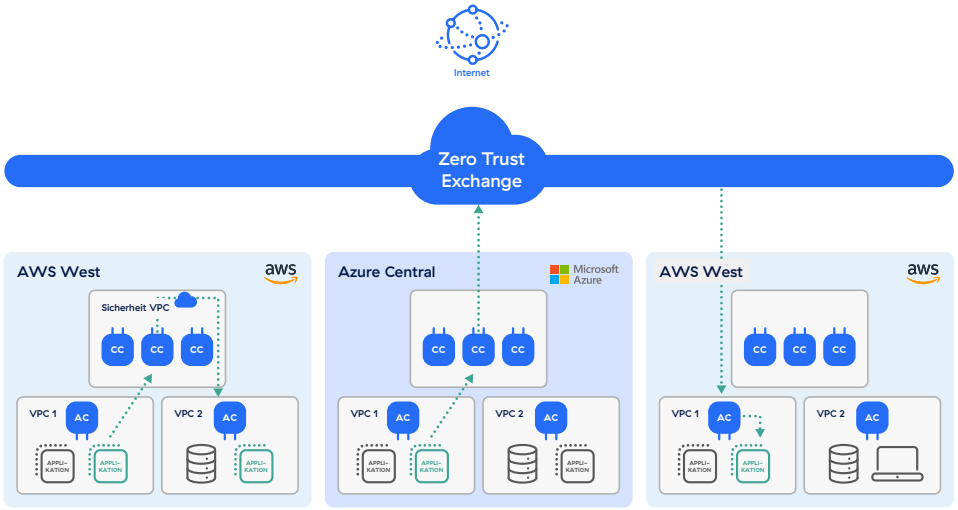
Kommunikation zwischen Workloads vereinfachen und schützen

Die Durchsetzung von Zero Trust für Cloud-Workloads erfordert auch eine sichere Konnektivität zwischen Workloads. Es ist wichtig, dass Workloads sowohl über mehrere Clouds hinweg als auch innerhalb einer einzelnen virtuellen privaten Cloud (VPC) kommunizieren können. Diese Kommunikation sollte über die zentrale Zero-Trust-Plattform laufen, auf der Sicherheitsrichtlinien angewendet werden und Verbindungsanfragen anhand von Identitätsprüfung und Kontextdaten autorisiert werden.

Insbesondere sollte ein Mechanismus vorhanden sein, der die Kommunikation zwischen Workloads erleichtert. Bei der VPC-zu-VPC-Konnektivität könnte der Datenverkehr von einer VPC zu einem privaten Service-Edge geleitet werden, von dem aus dann eine Verbindung zur Ziel-App (die sich in einer anderen VPC befindet) vermittelt würde. Für die Cloud-zu-Cloud-Konnektivität könnte der Datenverkehr an eine zentrale Zero-Trust-Plattform weitergeleitet werden, wo eine Verbindung zu einer Ziel-App in einer anderen Cloud hergestellt würde.

Zu den wichtigsten Funktionen, die zur Sicherung der Kommunikation zwischen Workloads erforderlich sind, gehören:

- Sichern der Multicloud- und Multiregion-Konnektivität
- Sicherung der Konnektivität zwischen VPCs/VNETs
- Eliminierung der Netzwerkangriffsfläche mit Zero Trust Network Access (ZTNA)
- Blockieren lateraler Bedrohungsbewegungen



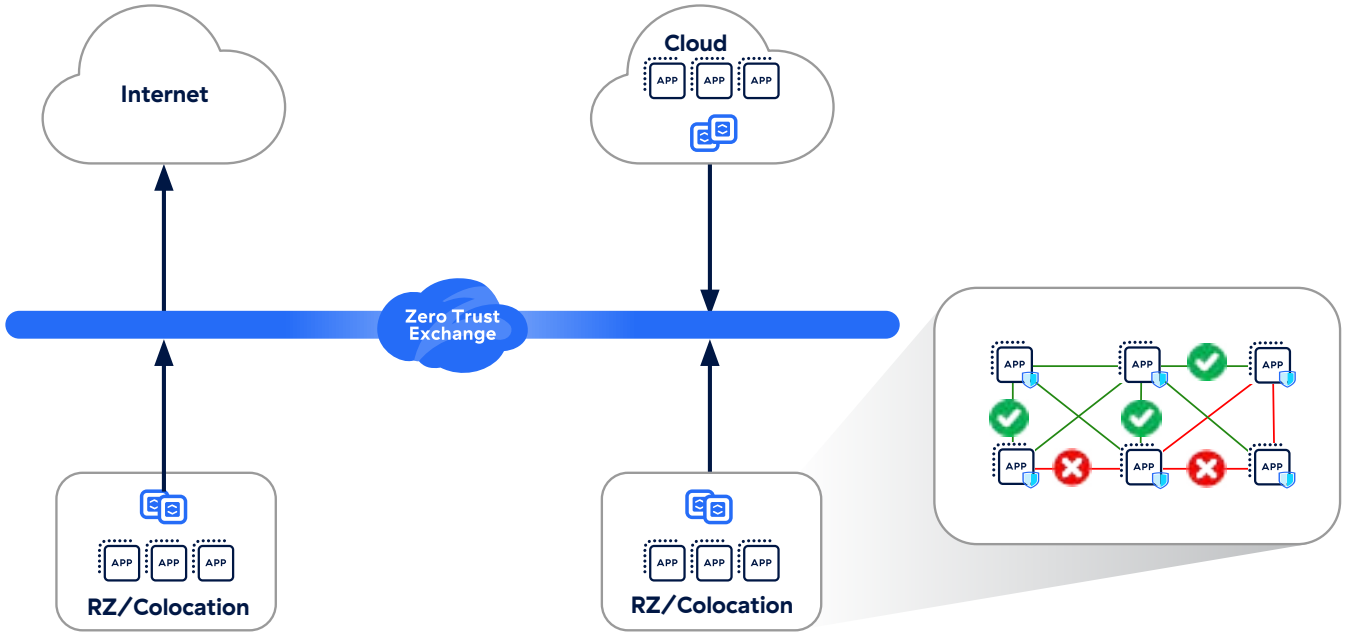
Granulare Mikrosegmentierung einfach gemacht

Mikrosegmentierung ist eine Kernkomponente der Zero-Trust-Sicherheit und verhindert die laterale Ausbreitung von Bedrohungen, indem Anwendungsgruppen oder Workloads basierend auf den Kommunikationsanforderungen einzelner Anwendungen in kleine Segmente unterteilt werden. Workloads dürfen zwar innerhalb ihrer eigenen Segmente kommunizieren, jedoch keine unbefugten Daten mit Workloads außerhalb dieser Segmente austauschen.

Durch Mikrosegmentierung können Zero-Trust-Richtlinien auf granularer Ebene im gesamten internen Netzwerk der Unternehmen und nicht nur an dessen Perimeter durchgesetzt werden. So wird ein konsistenter Schutz sowohl auf lokale als auch auf in der Cloud ausgeführte Workloads ausgedehnt.

Zu den wichtigsten Funktionen, die für die Mikrosegmentierung von Workloads erforderlich sind, gehören:

- KI-gestützte Ressourcenerkennung in Echtzeit
- Hostbasierte und nicht-hostbasierte Segmentierung
- Fähigkeit zur Segmentierung von Workloads innerhalb und zwischen VPCs/VNETs



Eine Zero-Trust-Lösung für Cloud-Workloads muss über mehrere Kernfunktionen verfügen:

Nr. 1: TLS/SSL-Überprüfung im großen Maßstab

Viele der gefährlichsten Bedrohungen verbergen sich direkt vor unseren Augen im verschlüsselten Traffic. Zu ihrer Erkennung benötigen Sie eine umfassende Plattform, die vollständige TLS/SSL-Überprüfung im großen Maßstab durchführt, ohne die Leistungseinschränkungen älterer Anwendungen.

Eine geeignete Lösung umfasst folgende Funktionen:

- **Unbegrenzte Kapazität** zur Überprüfung des gesamten TLS/SSL-Traffics aller User ohne Leistungseinbußen
- **Flexible Skalierbarkeit** basierend auf den Traffic-Anforderungen
- **Optimierte Zertifikatsverwaltung**
- **Granulare Richtlinienkontrolle**, die die Einhaltung von Vorschriften vereinfacht, indem verschlüsselter Userverkehr für Website-Kategorien wie Gesundheitswesen oder Bankwesen ausgeschlossen wird

Nr. 2: Robuste Funktionen zur Data Protection

Ein Defense-in-Depth-Ansatz zur Data Protection umfasst die Möglichkeit, Richtlinien zur Verhinderung von Datenverlust (Data Loss Prevention, DLP) in großem Maßstab durchzusetzen, ohne die Leistung zu beeinträchtigen. Dadurch entsteht eine zusätzliche Schutzschicht. Sollte eine Cloud-Workload jemals kompromittiert werden, steht immer noch ein Mechanismus zur Verfügung, um Richtlinien durchzusetzen und die Exfiltration von Daten zu verhindern.

Eine geeignete Lösung umfasst folgende Funktionen:

- **Optimiertes Dashboard**, in dem DLP-Richtlinien konfiguriert und verwaltet werden können
- **Erweiterte Datenverwaltungstechniken** wie Exact Data Management (EDM) und Optical Character Recognition (OCR)
- **Zuverlässige Inline-Überprüfung auch bei hohen Trafficvolumen**

Nr. 3: Erweiterte Funktionen zum Schutz vor Bedrohungen

Um die gefährlichsten komplexen Bedrohungen zu blockieren, muss eine Zero-Trust-basierte Sicherheitsplattform zum Schutz von Cloud-Workloads gewährleisten können, dass jedes Paket von jeder Workload lückenlos überprüft werden kann. Dies erfordert integrierte, ständig verfügbare TLS/SSL-Überprüfungsfunktionen sowie die Möglichkeit, detaillierte Richtlinien für den gesamten Datenverkehr durchzusetzen.

Darüber hinaus sollten Sie auf folgende Schlüsselfunktionen achten:

- **Integrierte Deception-Technologien** mit Decoys, Ködern und Honeypots zum Schutz Ihrer wertvollsten IT-Assets mit hoher Zuverlässigkeit und niedriger Fehlalarmquote
- **Cloud-Sandboxing,** um potenzielle Bedrohungen unter Quarantäne zu stellen und zu untersuchen, anstatt sie durchzulassen
- **Malware-Schutz**, der bekannte Ransomware, Spyware und Malware sowie neue Bedrohungen blockieren kann

Nr. 4: Umfassende hostbasierte Segmentierung

Durch Mikrosegmentierung wird die laterale Ausbreitung von Bedrohungen verhindert, um den potenziellen Schaden zu minimieren, den ein Cyber-Vorfall verursachen kann. Hostbasierte Mikrosegmentierung basiert auf Agents, die auf Endgeräten installiert werden, um eine wesentlich detailliertere Kontrolle und Sichtbarkeit zu bieten und so die Verwaltung der identitätsbasierten Segmentierung zu vereinfachen. Mithilfe eines Agents können Sie auf der Basis dynamischer, für Menschen verständlicher Richtlinien — anstelle von statischen Regeln auf Netzwerkebene — segmentieren.

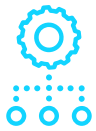
Konkret sollte eine geeignete Lösung folgende Funktionen umfassen:

- **Ressourcenerkennung in Echtzeit** mithilfe von KI, um Ihnen detaillierte Einblicke in alle Geräte, Services und Assets in Ihrem Unternehmensökosystem zu geben
- **Empfehlungen für Zero-Trust-Richtlinien** basierend auf der Verkehrsanalyse
- **Integration mit einer Zero-Trust-Plattform,** sodass Sie Ihre Umgebung an nur einem Ort schützen und segmentieren können, ohne mehrere Punktprodukte bereitstellen zu müssen

Die wichtigsten Anwendungsfälle zur Sicherung der Workload-Konnektivität

Eine auf Zero Trust basierende Lösung für die Workload-Konnektivität kann Unternehmen bei der Bewältigung verschiedener entscheidender Herausforderungen helfen. Dazu zählen insbesondere:

Sicherung des ausgehenden Traffics ins Internet
Wenn Anwendungen mit dem Internet oder SaaS-Anwendungen kommunizieren, muss der ausgehende Traffic auf Cyberangriffe und Datenlecks überprüft werden. Zscaler betreibt die weltweit größte Inline-Cloud-Sicherheitsplattform, die erweiterten Bedrohungsschutz im Cloud-Maßstab ohne Leistungseinbußen oder Beeinträchtigung der Servicequalität bietet.



Workload-Segmentierung
Mit der richtigen Workload-Kommunikationslösung ist ein granularer und methodischer Ansatz zur Workload-Segmentierung möglich. Dies vereinfacht die Anwendung von Richtlinien zur Steuerung der Konnektivität für Workloads über VPCs, Regionen sowie öffentliche und private Clouds hinweg.

Cloud-Migration
Dies ist für Unternehmen oft ein zeitaufwendiger und mühsamer Prozess. Sie müssen viele Faktoren berücksichtigen, einschließlich der Frage, welche Migrationsstrategie sie verfolgen sollen. Ist ein einfacher Wechsel sinnvoll oder sollten Apps durch Refactoring umgestaltet oder neu erstellt werden? Mit der richtigen Workload-Kommunikationslösung können Sie neu migrierte Cloud-Apps einfacher und sicherer verbinden.

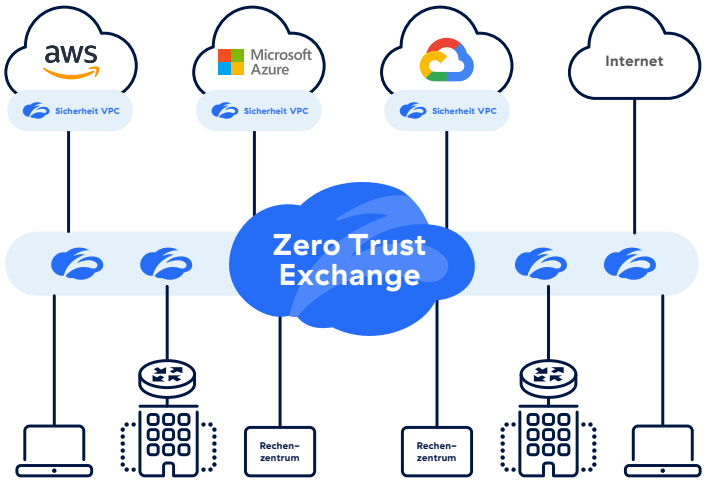
Fusionen und Übernahmen
Mit einer zukunftsfähigen Zero Trust-basierten Cloud-nativen Workload-Kommunikationslösung ist es möglich, einen sicheren netzwerkübergreifenden Anwendungszugriff bereitzustellen, ohne dass die Netzwerke für die Verbindung neu konzipiert und strukturiert werden müssen.

Zscaler Workload Communications löst das Problem

Suchen Sie nach einer End-to-End-Lösung, die all dies und noch mehr kann? Die Zscaler Zero Trust Exchange™ hat es möglich gemacht, die Workload-Kommunikation innerhalb einer einfachen, bewährten Direct-to-Cloud-Architektur völlig neu zu konzipieren.

Durch die Kombination von Zscaler Internet Access™ (ZIA) für die Kommunikation zwischen Workloads und Internet, Zscaler Private Access™ (ZPA) für die Kommunikation zwischen Workloads sowie Zero-Trust-Mikrosegmentierungsfunktionen ist Zscaler Workload Communications ein umfassender Ansatz zur Sicherung der Workload-Konnektivität in der Cloud und in lokalen Umgebungen. Gleichzeitig bleibt die Leistung erhalten, um Ihren Usern hervorragende Anwendererfahrungen zu bieten. Außerdem kann die Skalierbarkeit mit dem zukünftigen Ausbau Ihres Cloud-Ökosystems Schritt halten.

Zscaler Workload Communications bietet hochwirksame, auf Zero Trust basierende Cloud-Sicherheit, die sich entsprechend Ihren Anforderungen skalieren lässt. Dank der flexiblen Autoscaling-Funktionen kann das System problemlos mit steigenden Trafficvolumen umgehen. Die Zero Trust Exchange arbeitet bereits im Hyperscale-Bereich mit mehr als 150 Rechenzentren rund um den Globus. Zscaler übernimmt alle Updates automatisch für Sie. Die Infrastruktur ist nativ in die Sicherheitsinfrastruktur öffentlicher Cloud-Anbieter integriert und nutzt Funktionen wie Transit-Gateways und Load Balancer.



Darüber hinaus vereinfacht und zentralisiert Zscaler Workload Communications die Richtlinienverwaltung. Alle Richtlinien können in einer einzigen, zentralen und bedienerfreundlichen Konsole erstellt und aktualisiert werden. Die Durchsetzung erfolgt innerhalb der Zero Trust Exchange, wo entweder ZIA- oder ZPA-Richtlinien genutzt werden können, um eine vollständige Inhaltsprüfung und identitätsbasierte Kontrolle der Workload-Kommunikation zu ermöglichen. Von dort aus können die Nachrichten an jedes beliebige Ziel weitergeleitet werden, sei es das Internet oder andere private Unternehmensanwendungen in Cloud-Umgebungen. Richtlinien können problemlos im großen Maßstab angewendet werden, wenn Sie zusätzliche Workloads in der Cloud bereitstellen müssen.

Wenn Sie mehr über die Vorteile von Zscaler Workload Communications erfahren möchten, kontaktieren Sie uns noch heute. Weitere Informationen finden Sie auch auf der Webseite zu Zscaler Zero Trust Cloud Connectivity.

Experience your world, secured.™

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, resilienter 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. Informieren Sie sich auf **zscaler.com/de** oder folgen Sie uns auf Twitter unter **@zscaler**.

+1 408 533 0288

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

zscaler.com/de