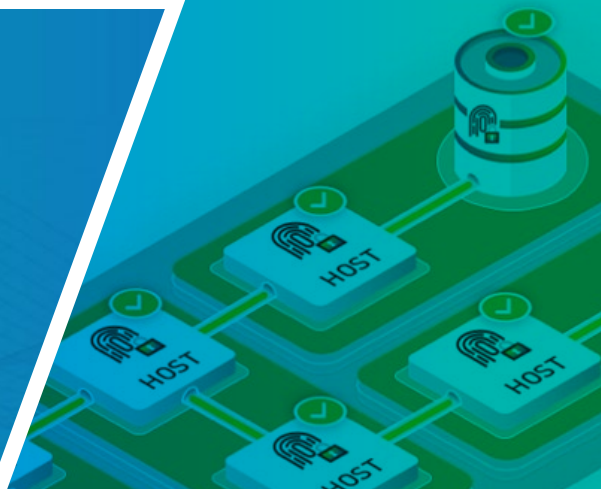
DATENBLATT

ZSCALER™ WORKLOAD SEGMENTATION

One-Click Zero Trust

Automatische Mikrosegmentierung für öffentliche Clouds und Rechenzentren



Mikrosegmentierung einfach gemacht

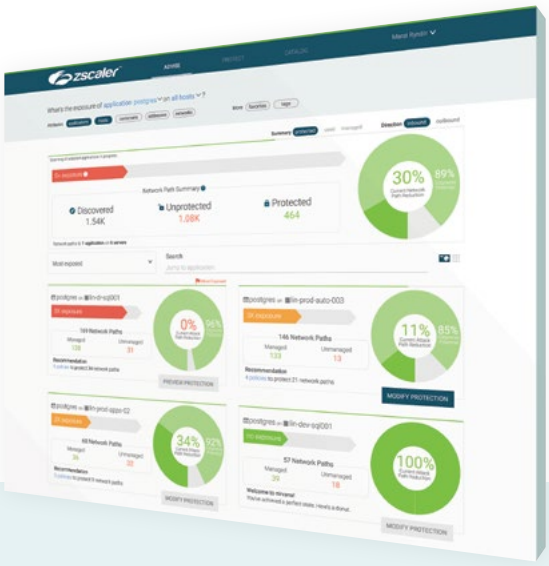
Cyberbedrohungen benötigen Angriffspfade, um anfällige Ziele zu erreichen. Am effektivsten lässt sich die Angriffsfläche, die ein Netzwerk bietet, durch Segmentierung reduzieren. Die Experten sind sich einig: Mikrosegmentierung zählt zu den wichtigsten Strategien zum Schutz von Workloads. Bislang überwogen jedoch die mit der Implementierung verbundenen Nachteile – hoher Zeit- und Kostenaufwand sowie Komplexität – gegenüber den Sicherheitsvorteilen einer effektiven Segmentierung.

Das ist jetzt anders.

Mit Zscaler Workload Segmentation steht Unternehmen eine neue, einfache Methode zur Mikrosegmentierung ihrer Umgebung mit einem einzigen Klick zur Verfügung. Zscaler Workload Segmentation deckt Risiken auf und wendet identitätsbasierten Schutz auf Workloads an, ohne dass architektonische Veränderungen am Netzwerk oder Neustarts erforderlich sind. Dadurch lassen sich nicht nur Risiken mindern, sondern auch der Verwaltungsaufwand reduzieren. Zscaler Workload Segmentation beruht auf einem Software-identitätsbasierten Modell und gewährleistet lückenlosen Schutz mit Richtlinien, die sich automatisch an die Umgebung anpassen, in der sie ausgeführt werden. Damit wird die Eliminierung von Angriffsflächen im Netzwerk so einfach wie noch nie.

Zscaler Workload Segmentation – Wertversprechen

- Ermöglichung vollständiger Transparenz jedweder lateralen Netzwerkkommunikationen
- Patentierte identitätsbasierte Richtlinien, die sich an Ihre dynamische Umgebung anpassen
- Maximale Sicherheit und Performance durch agentbasierten Schutz
- Mühelos Optimierung von Richtlinien zur Risikominderung und einfachen Verwaltung
- Nachweisbarer ROI für Sicherheitsinvestitionen



> „… durchaus denkbar, dass Zscaler Workload Segmentation über kurz oder lang in allen Unternehmen weltweit zum Einsatz kommt.
>
> goulston&storrs

Vorteile der anwendungsbezogenen Steuerung

Netzwerke in Cloud-Umgebungen und Rechenzentren enthalten jede Menge Daten, die für Cyberkriminelle attraktiv sind. Auch noch so starke Perimeterkontrollen können nicht verhindern, dass Cyberkriminelle durch Phishing oder eine andere Form des Social Engineering auf das Unternehmensnetzwerk zugreifen. Bei herkömmlichen netzwerkbasierten Sicherheitsstrategien braucht ein Angreifer nur Anmeldedaten zu stehlen oder sich über eine Sicherheitslücke Zugang zum Netzwerk zu verschaffen – und schon kann er Malware einschleusen und sich durch laterale Bewegungen innerhalb vertrauenswürdiger Netzwerkkommunikationspfade unbefugten Zugriff auf unternehmenskritische Anwendungen verschaffen. Ein kompromittiertes Netzwerk ist mehr als nur ein Ärgernis – es kann weitreichende finanzielle, rufschädigende und betriebliche Konsequenzen nach sich ziehen.
Zur Verhinderung unbefugter lateraler Kommunikation sind Sicherheitskontrollen erforderlich, die auf der *Verifizierung der Identität zugelassener Anwendungen basieren.*

Zscaler Workload Segmentation ermöglicht einen anwendungsbezogenen Ansatz zum Schutz von Netzwerken jeder Art mit Zero-Trust-Sicherheitskontrollen, die auf der Überprüfung der kryptografischen Identitätsattribute der kommunizierenden Software basieren.

Zero-Trust-Ansatz zur Stärkung der Sicherheit

Zscaler Workload Segmentation ersetzt das herkömmliche Sicherheitsmodell, bei dem Kommunikation basierend auf vertrauenswürdigen IP-Adressen, Ports und Protokollen zugelassen wird, durch einen Zero-Trust-Ansatz auf der Basis verifizierter Workload-Identitäten.
Unser Zero-Trust-Modell macht keinen Unterschied zwischen interner Kommunikation und dem Internet: Beide sind potenziell feindselig und voller Bedrohungen. Nur Anwendungen und Services, die anhand ihrer kryptografischen Identität verifiziert wurden, dürfen Kommunikationen senden und empfangen. Das Ergebnis ist eine Stärkung der Sicherheit in sämtlichen Umgebungen.

Patentierte identitätsbasierte Auto-Segmentierung

Die Legacy-Mikrosegmentierung umfasst mehrere Schritte und kann insgesamt Monate in Anspruch nehmen. Mit Zscaler Workload Segmentation ist die Mikrosegmentierung mit einem einzigen Klick in Minutenschnelle abgeschlossen – vom Asset-Inventar über die Zuordnung von Datenflüssen bis hin zur Implementierung der durchzusetzenden Richtlinien.

Zscaler Workload Segmentation schützt unternehmenskritische Daten und Anwendungen in der Hybrid-Cloud über eine grundlegend neue Kontrollebene: die Software-Identität. Sämtliche Software in einer von Zscaler Workload Segmentation verwalteten Umgebung wird anhand einer Kombination aus kryptografischen Identitätsattributen mit einem Fingerabdruck versehen. Alle Entscheidungen bezüglich Zugriffskontrolle werden auf der Basis der Software-Identität getroffen. Ungeachtet früherer Berechtigungen darf entsprechend unserem Zero-Trust-Modell eine Software nur kommunizieren, wenn sie verifiziert werden kann. Dadurch kann unabhängig von Veränderungen am Netzwerk höchstmöglicher Schutz für Workloads gewährleistet werden.

Schutz von neu eingeführten Anwendungen durch automatische Neusegmentierung

Auto-Segmentierung eignet sich ideal zur Beschleunigung der Erstbereitstellung von Mikrosegmentierung. Ebenso wichtig ist jedoch, dass auch der Schutz neu eingeführter Anwendungen gewährleistet wird. Durch diese neuen Anwendungen entstehen möglicherweise völlig neue Kommunikationspfade bzw. Interaktionen mit vorhandenen Anwendungs-Services, die alle gesichert werden müssen.
Durch automatische Neusegmentierung mit einem einzigen Klick macht Zscaler Workload Segmentation auch den Schutz dieser neuen Anwendungen unglaublich einfach. Basierend auf der bestehenden Segmentierung empfiehlt Zscaler Workload Segmentation neue oder modifizierte Richtlinien zur Sicherung der neu hinzugekommenen Kommunikationen zwischen Anwendungen – alles mit einem Klick. Mit der Kombination aus automatischer Segmentierung und Neusegmentierung ist Ihre dynamische Umgebung jederzeit zuverlässig gesichert.

Diese neue Methodik bedeutet, dass sich die Sicherheitskontrolle an jede Umgebung anpasst und weniger Richtlinien verwaltet werden müssen. Durch Zero-Trust-Autosegmentierung gewährleistet Zscaler Workload Segmentation stärkeren, vereinfachten und skalierbaren Schutz für Hybrid-Cloud-Umgebungen mit sechs Unterscheidungsmerkmalen:

Automatische Richtlinienerstellung

Risikominderung durch Richtlinien-Komprimierung

Nachweisbare Sicherheitsergebnisse

Verifizierung der Software-Identität anhand kryptografischer Attribute

Automatische Anpassung an Aktualisierungen und Änderungen der Anwendungen

Tools zur Sicherheitsüberwachung werden mit Anwendungsdaten aktualisiert

Zero Trust Identity

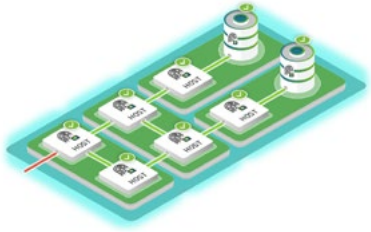
Die Technologie, die der automatischen Mikrosegmentierung von Zscaler Workload Segmentation zugrunde liegt, basiert auf Zero Trust Identity (ZTID). Zu den Attributen, die die Identität von Workloads ausmachen, zählen u. a. der SHA256-Hash, der Fuzzy-Hash, die Signierung der ausführbaren Datei, PE-Header-Werte, UID, CPU-Seriennummern und der Name des bereitgestellten Hosts. Auf der Basis dieser eindeutigen Identitäten werden mithilfe von Machine Learning Richtlinien-Empfehlungen erstellt und Entscheidungen bezüglich der Zugangskontrolle getroffen. Alle Richtlinien im Rahmen von Zscaler Workload Segmentation basieren auf dem „Zero Trust"-Prinzip. Entsprechend darf keine Software, die nicht vom ZTID verifiziert werden kann, in den Netzwerken kommunizieren. Dadurch ist mehr Sicherheit ohne Abstriche bei der betrieblichen Effizienz des Netzwerks gewährleistet.

Einfacher in der Umsetzung

Die Mikrosegmentierung von Umgebungen erfolgt in Minutenschnelle mit nur einem Klick. Geschäftsanwendungen sind automatisch gesichert und betriebsbereit. Es sind keine Änderungen am Netzwerk und keine manuelle Erstellung oder Aktualisierung von Richtlinien erforderlich – und langwierige Deployments gehören der Vergangenheit an.

Stärker bei der Sicherheit

Die Bereichsgrenzen werden nicht basierend auf IP-Adressen, sondern auf Abhängigkeiten zwischen der kommunizierenden Software definiert. Durch Überprüfung der Software-Identität wird sichergestellt, dass nur legitime Geschäftsanwendungen in Cloud-Umgebungen und Rechenzentren kommunizieren. So lässt sich der Verbreitung von Malware und dem Missbrauch von Administrator-Tools ein Riegel vorschieben.



Skalierbar für DevOps

Beim Deployment von Workloads kann der für reibungslose Geschäftsabläufe erforderliche Zugriff gewährleistet werden. Die Anpassung der Richtlinien im Rahmen von Zscaler Workload Segmentation für alle VMs und Kubernetes-Container – On-Premise oder in der öffentlichen Cloud – erfolgt automatisch mit der Skalierung der Umgebung.

Zentrale Verwaltung von Multi- und Hybrid-Cloud-Umgebungen

Zscaler Workload Segmentation gewährleistet umfassende Unterstützung für alle Umgebungen von On-Premise-Hardware über virtualisierte Private Cloud oder öffentliche Cloud bis hin zu beliebigen Kombinationen. Dabei kann es sich um statische oder auch hochdynamische Umgebungen handeln. Zscaler Workload Segmentation unterstützt 10 Linux-Distributionen (mit über 800 Patch-Levels, die bis zu 2.6 zurückreichen), Windows 7 und aufwärts sowie alle Versionen von Windows Server. Zusätzlich werden Container-Umgebungen wie Kubernetes, Docker und AWS Elastic Container Service (ECS) unterstützt.

Die kontinuierlich adaptive Plattform sowie die in Zscaler Workload Segmentation inbegriffenen Produkte sind API-gesteuert. Zscaler Workload Segmentation kann zur automatischen Segmentierung mit einem Klick in vorhandene Sicherheitstools und DevOps-Prozesse integriert werden.

Linux Windows Windows Server kubernetes docker Amazon ECS

Azure Google Cloud Platform aws vmware

Zscaler Workload Segmentation – Anwendungsfälle

ZERO TRUST ZUM SCHUTZ VON CLOUD-WORKLOADS

Alle geschäftskritischen Anwendungen in unterschiedlichen Cloud-Umgebungen können über eine zentrale Plattform gesichert werden.

ZERO-TRUST-MIKROSEGMENTIERUNG ZUM ERKENNEN VON COMPLIANCE-VERSTÖSSEN

Durch Segmentierung der Anwendungen in „sichere Zonen" lassen sich Compliance-Verstöße im Voraus erkennen und verhindern.

DATENFLUSSZUORDNUNG FÜR MEHR TRANSPARENZ

Durch Visualisierung der Anwendungstopologie werden Änderungen unmittelbar sichtbar.

CONTAINER-SICHERHEIT

Anwendungen in vorübergehenden Produktivumgebungen können ohne Unterbrechungen des CI-/CD-Workflows geschützt werden.

EREIGNISKORRELATIONUNDSICHERHEITS-ÜBERWACHUNG

Kommunikationsprotokolle der Anwendungen können ins SIEM eingespeist werden, um die Priorisierung von Maßnahmen zur Fehlerbehebung zu unterstützen.

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Zscaler Zero Trust Exchange schützt tausende Kunden mittels sicherer Verbindungen zwischen Benutzern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Bei der SASE-basierten Zero Trust Exchange, die in 150 Rechenzentren auf der ganzen Welt verfügbar ist, handelt es sich um die größte Inline-Cloud-Sicherheitsplattform der Welt.

zscaler™

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