DATENBLATT

Zscaler Microsegmentation

Herausforderungen bei herkömmlicher Mikrosegmentierung

Viele Unternehmen setzen beim Schutz ihrer Workloads auf Legacy-Segmentierungsarchitekturen. Diese Architekturen sind unzureichend: Ihre Bereitstellung ist komplex, sie vergrößern die Angriffsfläche, verstärken die laterale Bewegung und erhöhen die Betriebskosten.

- Die Erstellung einer genauen Bestandsaufnahme ist eine Herausforderung, insbesondere bei Ressourcen in der Cloud, wo sie dynamisch erstellt und gelöscht werden.
- Lösungen wie Firewalls erweitern das Netzwerk auf Workloads und Server und erhöhen so das Risiko lateraler Bewegungen.
- Ein Patchwork aus virtuellen Appliances, Betriebstools und nicht standardisierten Richtlinien führt zu bekannten und unbekannten Lücken im Sicherheitsschutz und erhöht so das Risiko.
- Die Bereitstellung userdefinierter Segmentierungstools von Drittanbietern ist komplex und die Durchsetzung der Sicherheitsrichtlinien des Unternehmens erfolgt inkonsistent.

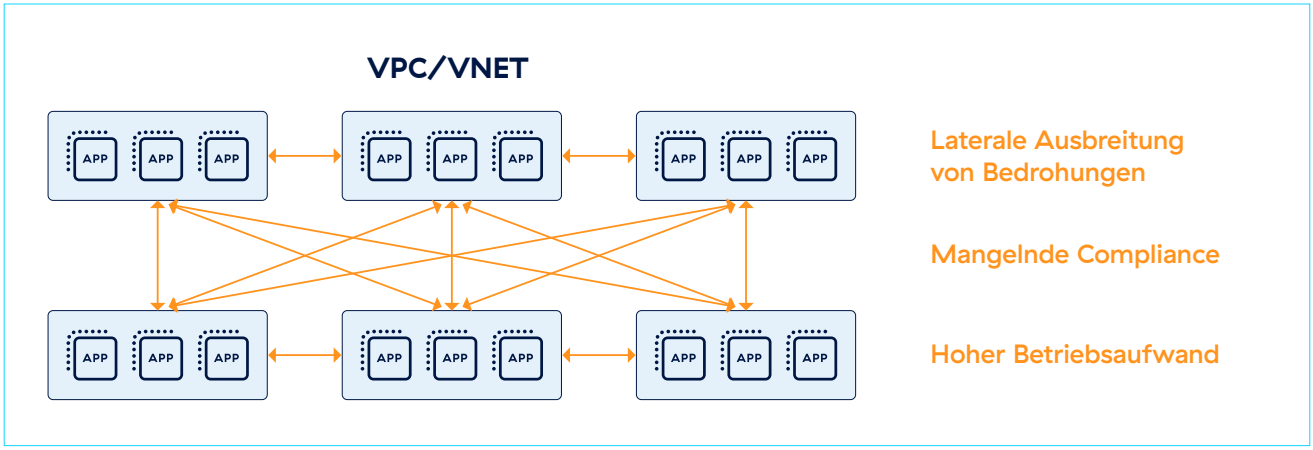

Abb. 1: Herkömmliche Workload-Schutzarchitekturen reichen nicht aus, um die Ausbreitung lateraler Bedrohungen zu stoppen

Erweitern Sie die Zero-Trust-Architektur, um Workloads in öffentlichen Clouds und lokalen Rechenzentren zu segmentieren

Die hostbasierte Mikrosegmentierung bewältigt diese Herausforderungen, indem sie das Netzwerk in kleinere, besser kontrollierbare Segmente aufteilt. Sie setzt Sicherheitsregeln für jedes Segment durch und genehmigt nur unbedingt erforderliche Zugriffsanforderungen. Auf diese Weise bleibt der Rest des Netzwerks sicher, wenn ein Segment angegriffen wird. Angesichts immer ausgefeilterer Cyberbedrohungen ist es offensichtlich, dass einfache Perimeterschutzmaßnahmen diese raffinierten Angriffe nicht mehr stoppen können.

Zscaler Microsegmentation gewährleistet:

Echtzeiterkennung und -transparenz von Assets: Erhalten Sie ein Inventar der Assets in Ihrer gesamten Infrastruktur.

- Erkennung von Assets nahezu in Echtzeit. Erhalten Sie ein Inventar aller Assets basierend auf userdefinierten Tags und Cloud-Attributen (VPC/VNET) oder Netzwerkobjekten (IP/Subnetz).
- Erhalten Sie Einblick in Ressourcen in mehreren öffentlichen Clouds, Rechenzentren und Co-Locations in einer einzigen Konsole.

Automatisierte Richtlinienempfehlung: Stellen Sie sicher, dass alle Assets durch eine Sicherheitsrichtlinie abgedeckt sind.

- Erhalten Sie Richtlinienempfehlungen zum Segmentieren von Arbeitsabläufen basierend auf der Verkehrsflussanalyse.
- Erhalten Sie proaktive Richtlinienvorschläge zum Schutz nicht segmentierter Ressourcen.

Granulare Richtliniendurchsetzung: Stoppen Sie die laterale Ausbreitung von Bedrohungen.

- Erzwingen Sie Kontrollen auf Hostebene, um den Zugriff zu beschränken.
- Setzen Sie konsistente Sicherheitsrichtlinien für alle Ressourcen in Rechenzentren und öffentlichen Cloud-Umgebungen durch.

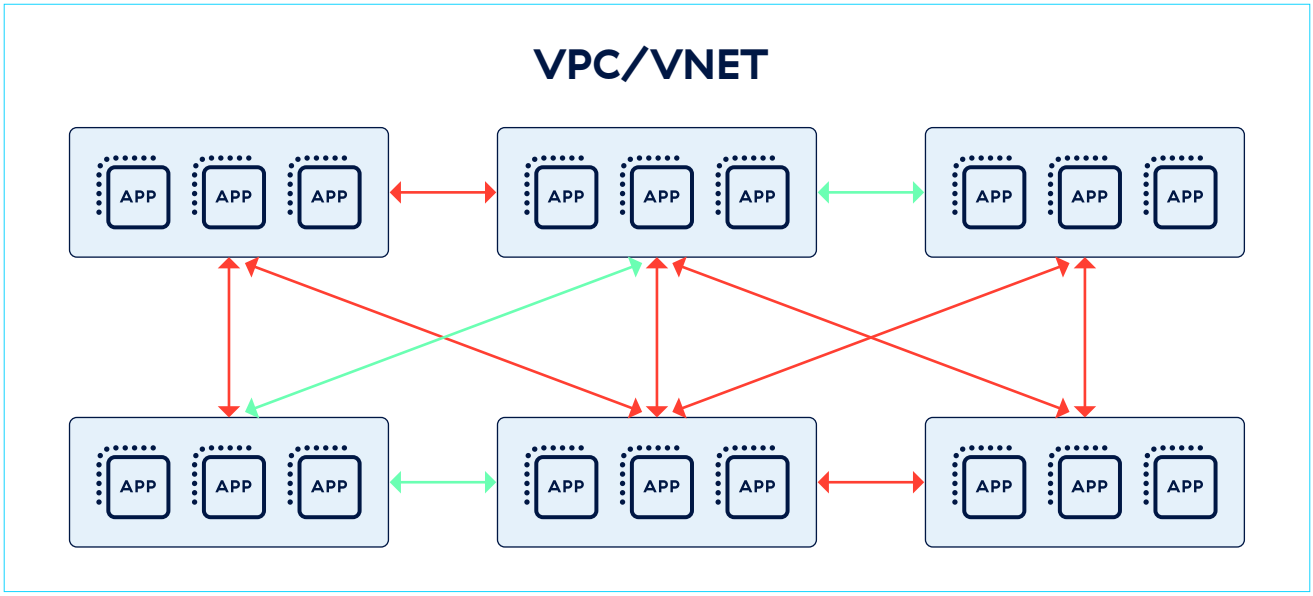

Abb. 2: Zscaler Microsegmentation bietet Zero-Trust-basierte, hostbasierte Segmentierung

Mikrosegmentierungsfunktionen von Zscaler

Funktion	Details
Abdeckung für öffentliche Clouds und lokale Standorte	Sichern Sie Workloads in AWS, Microsoft Azure, mit zusätzlicher Unterstützung für lokale Rechenzentrumsserver.
Host-Inventar	Erhalten Sie Einblick in Ihre Cloud-Workloads, einschließlich Hostdetails, Cloud-Umgebung und userdefinierter Tags.
Datenfluss-Transparenz	Erhalten Sie detaillierte Einblicke in Datenflüsse, einschließlich 5-Tupel-Details, Anwendungsname und Anwendungspfad.
Visualisierung	Erhalten Sie eine interaktive Karte der Datenflüsse zwischen Anwendungsressourcen in der Umgebung.
Ressourcenrichtlinien	Erstellen und erzwingen Sie Richtlinien zwischen Ihren Anwendungsressourcen.
Anwendungsbereiche	Kontrollieren Sie den Umfang der Richtlinienregeln basierend auf Anwendungszonen oder Umgebungen.
Vereinfachte Agent-Upgrades	Aktualisieren Sie Zscaler Microsegmentation-Agenten gruppenweise mithilfe von Versionsprofilen.
Analyse-Dashboard	Analyse-Dashboards, einschließlich der Top-N-Ressourcen als Initiatoren, Empfänger und Datenflüsse zum Internet basierend auf beobachteten Datenfluss-Protokollen.
Umfassende Plattformunterstützung	Ressourcenschonende Agents können auf gängigen Betriebssystemen, einschließlich Windows und Linux, installiert werden.
Protokoll-Streaming	Konsolidieren Sie mit dem Zscaler Log Streaming Service Protokolle aller Workloads und Server weltweit in einem von Ihrem Unternehmen festgelegten zentralen Repository. Administratoren können Datenfluss-Protokolldaten von Workloads in Echtzeit anzeigen und auswerten.

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