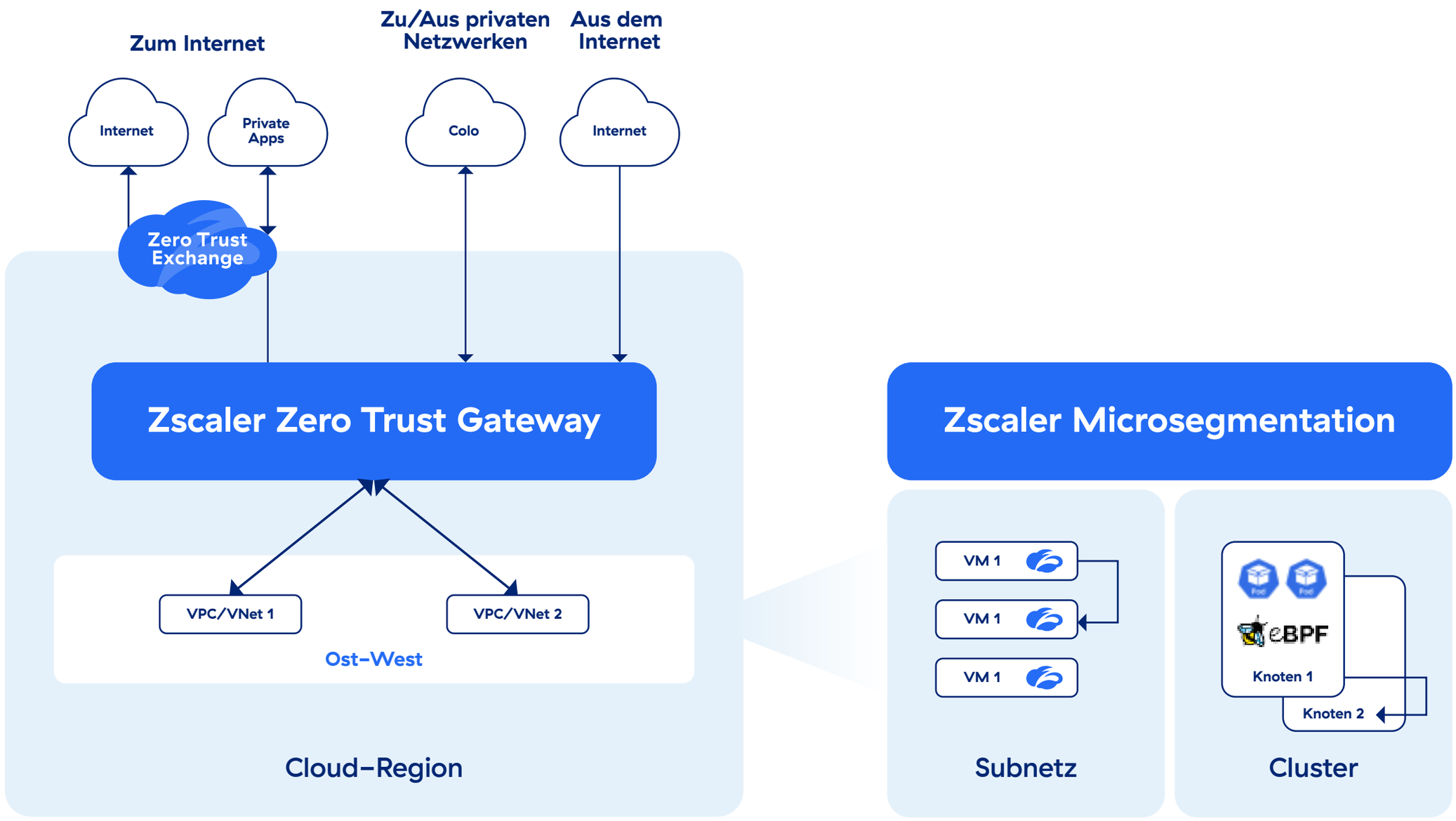
# Zero Trust Cloud

## Alle Workloads in der Cloud einfach und sicher verbinden.

DATENBLATT

Die digitale Transformation hat das Multicloud-Zeitalter eingeläutet — und damit eine wahre Flut an Workloads. Um erfolgreich zu bleiben, brauchen Sie lückenlose Transparenz über diese Ressourcen. Darüber hinaus, müssen Angriffe und Datenverluste konsequent verhindert werden.

Traditionelle Lösungen wie Firewalls und IPSec-VPNs stammen aus einer anderen Zeit — und genau das sieht man ihnen an. Sie geben Ihnen keine Echtzeiteinblicke in Ihre Ressourcen, schützen ungleichmäßig, erweitern die Angriffsfläche und begünstigen laterale Bewegungen. Dies erhöht zwangsläufig die betriebliche Komplexität und die Kosten.




Schützen Sie alle Traffic-Pfade mit Zero Trust Gateway/Connectors und Zscaler Microsegmentation.

Zero Trust Cloud bringt ganzheitliche Sicherheit in Ihre Multicloud-Umgebung. Die Lösung verschafft Ihnen volle Transparenz: Metadaten liegen sofort vor, Prozesse werden in Echtzeit sichtbar und Ihr Ressourcen-Inventar bleibt jederzeit exakt. Bedrohungen und Datenrisiken werden über alle Verbindungswege und Clouds hinweg einheitlich abgewehrt und Sie reduzieren Ihre Kosten, weil alles über eine Plattform läuft. Für umfassende Transparenz und Kontrolle über Microflows aus VMs oder Containern bietet die Lösung eine intelligente, hostbasierte Mikrosegmentierung.

# Erweiterung der Zero-Trust-Architektur auf Ihre Multicloud-Umgebung

**Mit Zero Trust Cloud profitieren Sie von Funktionen, die Ihren Sicherheitsstatus entscheidend stärken:**

## ECHTZEIT-TRANSPARENZ ÜBER CLOUD-RESSOURCEN

Mit Zero Trust Cloud erhalten Sie Echtzeit-Einblicke in Ihre Cloud-Ressourcen.

- **Sofortige Metadatenerfassung:** Integriert sich nahtlos in Ihre Cloud-Infrastruktur und erfasst automatisch Metadaten (Tags, Labels, Attribute), sobald Ressourcen erstellt, geändert oder gelöscht werden.
- **Detaillierte Einblicke auf Prozessebene:** Mit den Mikrosegmentierungs-Agents von Zscaler erhalten Sie granulare Metadaten zu einzelnen Prozessen in VMs und Containern.
- **Genaues Ressourcen-Inventar:** Erstellt automatisch ein detailliertes und präzises Inventar von VPCs/VNets, Subnetzen und VMs/EC2-Instanzen auf Regionenebene — ganz ohne manuellen Aufwand.

## KONSISTENTE, UMFASSENDE BEDROHUNGSABWEHR UND DATA PROTECTION

Durchsetzung einheitlicher Sicherheitsrichtlinien in einer Multicloud-Umgebung

- **Umfassender Schutz für alle Traffic-Pfade:** Eingehend, ausgehend, Ost-West, private Netzwerke und Microflows
- **TLS-Überprüfung und Bedrohungsschutz** im Cloud-Maßstab zur Abwehr von Zero-Day-Angriffen
- **Inline-Datenschutz** ur Verhinderung von Datenverlusten

## GERINGERE KOMPLEXITÄT UND KOSTEN

Ganzheitliche Sicherheitsplattform zum Schutz von Workloads in sämtlichen Cloud-Umgebungen

- **Absicherung von Workloads** aller gängigen Cloud-Service-Provider, einschließlich AWS, Azure und GCP, mit einer einheitlichen Plattform
- **Automatische Bereitstellung von Sicherheitskontrollen** durch programmierbare Schnittstellen, einschließlich Zscaler-APIs, Hashicorp Terraform und AWS CloudFormation
- **Unterstützung von Verbindungen von Cloud zu Cloud**, von Cloud zu Rechenzentrum, von Region zu Region, VPC/VNet zu VPC/VNet, Subnetz zu Subnetz und zwischen Hosts oder Knoten

## SICHERE UNTERNEHMENSKRITISCHE ANWENDUNGEN

Erfüllen Sie regulatorische Anforderungen und Compliance-Vorgaben und erhöhen Sie die Sicherheit Ihrer Workloads durch hostbasierte Mikrosegmentierung.

- **Prozesstransparenz:** Gewinnen Sie granulare Einblicke in Cloud-Ressourcen auf der Ebene einzelner Prozesse.
- **Automatisierte Ressourcengruppierung:** Maschinelles Lernen empfiehlt und definiert automatisch die optimalen Ressourcensegmente, basierend auf Analyse der Traffic-Flüsse.
- **Strikte Durchsetzung minimaler Zugriffsrechte:** Wenden Sie granulare Sicherheitsregeln für jedes Segment an, gewähren Sie nur den notwendigen Zugriff und begrenzen Sie mögliche laterale Bewegungen.

# Zero Trust Gateway/Connector: Funktionen

| EDITION | DETAILS |
|---|---|
| **Erweitert** | • TLS/SSL-Überprüfung<br>• Cloud-Firewall (Standard)<br>• Advanced Threat Protection<br>• NSS-Protokollfeed (Keine Protokollwiederherstellung)<br>• Cloud-zu-Cloud-Streaming<br>• Grundlegender DNS-Schutz<br>• Dateikontrolle<br>• Dynamische, risikobasierte Zugriffs- und Sicherheitsrichtlinien<br>• SaaS-Sicherheit (CASB Standard)<br>• Workload-zu-Workload-Segmentierung (ZPA)<br>• Anwendungserkennung (ZPA)<br>• Datenschutz (Überwachungsmodus)<br>• Zscaler-Quell-IP-Verankerung |
| **Advanced Plus** | • Funktionsumfang der Workloads Advanced Edition<br>• Absicherung von Workloads gegenüber dem Internet<br>• IPS, Datenschutz<br>• NSS-Protokollfeed (Mit Protokollwiederherstellung)<br>• Erweiterter DNS-Schutz<br>• Cloud-Sandbox (Advanced)<br>• Benutzerdefiniertes Root-Zertifikat<br>• SaaS-Sicherheit<br>• Cloud-Firewall (Advanced)<br>• Datenschutz (Inline)<br>• Exact Data Match (EDM)<br>• Indexed Document Match (IDM)<br>• Optical Character  Recognition (OCR) |

# Zscaler Microsegmentation: Funktionen

| EDITION | DETAILS |
|---|---|
| **Erweitert** | • Unterstützte Plattformen: Windows, Linux und Kubernetes (Amazon EKS)<br>• Einblick in Ihre Cloud-Workloads (AWS, Azure, GCP)<br>• Transparenz über Traffic-Flüsse einschließlich Anwendungsdetails<br>• Übersicht der Anwendungsabhängigkeiten<br>• Richtliniendurchsetzung<br>• Anwendungszonen für erweiterte Richtlinienbereiche<br>• Integrierte Agent-Aktualisierungen mithilfe von Versionsprofilen<br>• Erweiterte Traffic-Analyse<br>• Integration mit SIEM mittels Log Streaming Service (LSS)<br>• Workload Discovery Service — Integration von Zero Trust Gateway/Connector für Echtzeit-Transparenz über Multicloud-Metadaten |

**Über Zscaler**
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler 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 Datenverlusten. Als weltweit größte Inline-Cloud-Sicherheitsplattform wird die SASE-basierte Zero Trust Exchange™ in über 150 Rechenzentren auf der ganzen Welt bereitgestellt. Weitere Informationen erhalten Sie auf **zscaler.com/de**. Gerne können Sie uns auch auf X folgen **@zscaler**.



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

zscaler™

**Zero Trust Everywhere**