DATENBLATT

Zero Trust Cloud

Sichern Sie den Workload-zu-Internet- und Workload-zu-Workload-Verkehr für Ihre Cloud-Workloads mit der Leistungsfähigkeit der Zscaler Zero Trust Exchange™.

Die digitale Transformation treibt die Nutzung von Workloads in einer breiten Palette von lokalen, privaten und öffentlichen Cloud-Infrastrukturumgebungen voran. Diese Workloads spielen für die Betriebsabläufe Ihres Unternehmens eine wichtige Rolle und müssen unbedingt vor Cyberangriffen und Datenverlusten geschützt werden.

Legacy-Architekturen sind dieser Aufgabe nicht gewachsen: Sie bieten keinen einheitlichen Bedrohungsschutz und Data Protection, vergrößern die Angriffsfläche, verstärken das Risiko lateraler Bewegungen und erhöhen die betriebliche Komplexität und die Kosten.

Die Zscaler Zero Trust Cloud vereinfacht die Sicherheit hybrider Workloads radikal. Der ausgehende Traffic von Workloads zum Internet bzw. zu anderen Workloads über öffentliche Clouds und lokale Rechenzentren für Ihre unternehmenskritischen Workloads und Server wird mit der Leistung der Zero Trust Exchange geschützt.

Zero Trust Cloud gewährleistet konsistenten Bedrohungsschutz und Data Protection, eliminiert die Angriffsfläche, stoppt laterale Bewegungen, reduziert die Komplexität und senkt die Betriebskosten.

> “Mit Workload Communications von Zscaler können wir Sicherheitsrichtlinien für User und Anwendungen ganz einfach standardisieren, und zwar unabhängig von deren jeweiligem Standort bzw. der Hosting-Umgebung.”
>
> **Rui Cabeço,** Global Outbound Connectivity Lead, Siemens

Herausforderungen mit Legacy-Workload- und Serversicherheit

Viele Unternehmen setzen beim Schutz ihrer Cloud-Workloads weiterhin auf Legacy-Architekturen: Dabei kommt zumeist eine Kombination mehrerer Aktionen zum Einsatz:

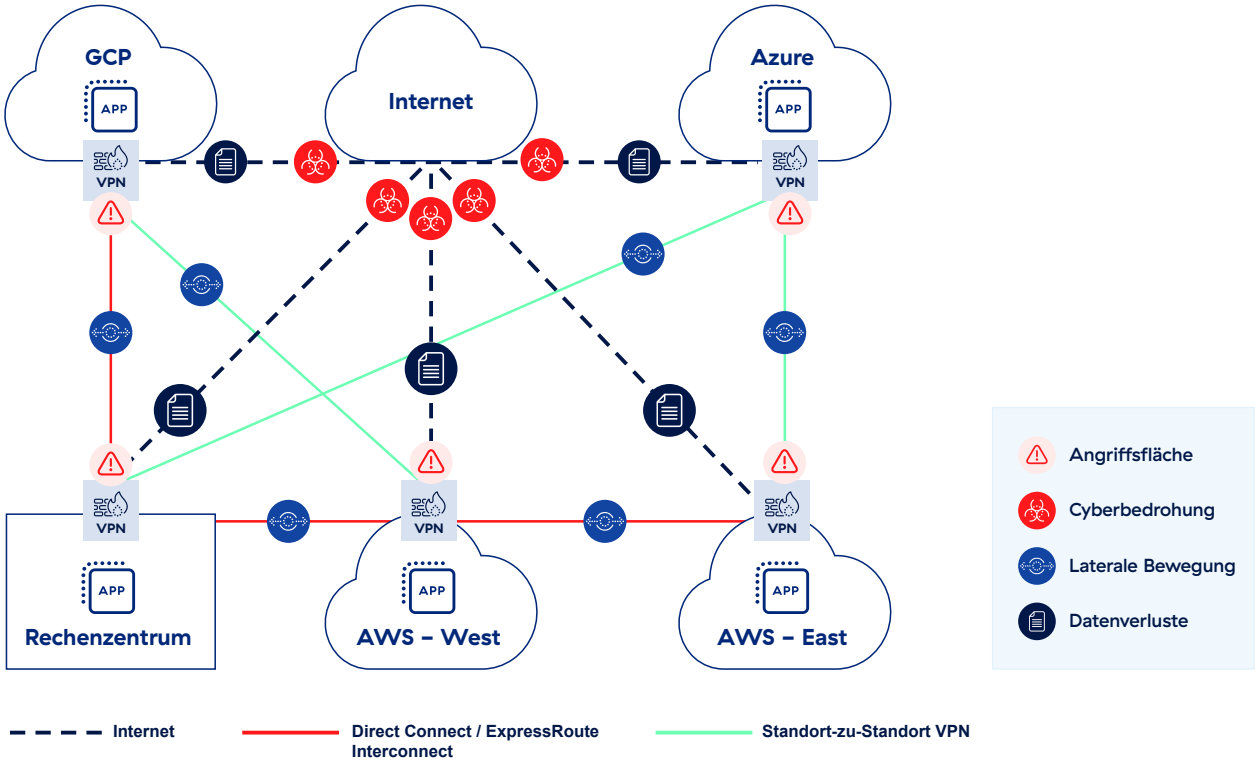
Native Sicherheitslösungen, die von öffentlichen Cloud-Dienstanbietern angeboten werden

Drittanbieter-Tools (Firewall, VPN, TLS/SSL-Überprüfung, DLP usw.) als zusätzlichen Schutz

Backhauling des Traffics zur lokalen Netzwerksicherheitsinfrastruktur zur Überprüfung und zum Schutz

Die Verwendung dieser Methoden bringt eine Reihe von Herausforderungen mit sich:

- **Erhöhte laterale Bewegung und Angriffsfläche.** Lösungen wie Firewalls erweitern das Netzwerk auf Workloads und Server und erhöhen so das Risiko lateraler Bewegung. Jede internetseitige Firewall vergrößert auch die Angriffsfläche. Dies kann das Internet auf verschiedene Clouds und lokale Umgebungen ausdehnen. Darüber hinaus führt ein Flickenteppich aus virtuellen Appliances, Betriebstools und nicht standardmäßigen Richtlinien sowohl bekannte als auch unbekannte Lücken in der Sicherheitsabdeckung ein und erhöht so das Sicherheitsrisiko.
- **Lücken in der TLS-Transparenz.** Die TLS-Prüfung kann erhebliche Rechenressourcen beanspruchen und Leistungseinbußen bei ihrer Aktivierung mit sich bringen. Die Verwaltung verteilter Zertifikate oder das Anwenden von Ausnahmen auf fixierte Workloads schafft betriebliche Herausforderungen. Darüber hinaus führt dies häufig zu höheren Kosten für die Cybersicherheitsinfrastruktur, um die Skalierung zu unterstützen.
- **Erhöhte Komplexität und schlechte Leistung.** Da herkömmliche Netzwerk- und Sicherheitslösungen nicht für Cloud-Workloads entwickelt wurden, müssen Einzelprodukte wie virtuelle Firewalls, Proxys und NAT-Gateways integriert werden. Einige Lösungen verwenden möglicherweise separate VMs für jede Sicherheitsfunktion, was zu einer sequentiellen Inspektion im Fließbandstil führt und die Latenz erhöht. Dies führt zu erheblichen betrieblichen Komplexitäten, wenn es in Multicloud-Umgebungen angewendet wird.
- **Hohe Kosten.** Die Verwendung veralteter Netzwerksicherheitsprodukte (z. B. Firewalls, IPS, Router), die Überbereitstellung der Netzwerksicherheitsinfrastruktur zum Ausgleich mangelnder Skalierbarkeit und die zunehmende Nutzung nativer Cloud-Dienste tragen zu höheren Anschaffungs- und Betriebskosten bei.
- **Fehlende gemeinsame Protokollierung.** Gesetzliche und behördliche Auflagen können Unternehmen dazu verpflichten, Protokolle über längere Zeiträume hinweg zu speichern. Der Zugriff auf diese Protokolle aus verschiedenen Cloud-Umgebungen und ihre Speicherung in einer zentralen SIEM-Infrastruktur kann komplex und teuer sein.



Erweitern Sie die Zero-Trust-Architektur auf öffentliche Clouds und lokale Rechenzentren

Zero Trust Cloud eliminiert die Angriffsfläche des Netzwerks, indem Workloads und Server über eine Zero-Trust-Architektur mit dem Internet und privaten Unternehmensanwendungen verbunden werden. Dies vereinfacht die Konnektivität erheblich, indem die Abhängigkeit Ihres Unternehmens von Legacy-Lösungen wie Firewalls reduziert wird. Gleichzeitig wird eine flexible Weiterleitung ermöglicht und die Richtlinienverwaltung mit dem bewährten Richtlinienrahmen von Zscaler Internet Access™ (ZIA) und Zscaler Private Access™ (ZPA) vereinfacht.

Möglich wird dies alles durch die Zero Trust Exchange, die im Hyperscale-Modus betrieben wird und jede Zunahme des Workload- oder Server-Traffics durch elastische, horizontale Skalierung bewältigen kann. Mit Zero Trust Cloud wird der gesamte ausgehende Workload- und Server-Traffic an die Zero Trust Exchange weitergeleitet, wo Sicherheitsrichtlinien für die vollständige TLS/SSL-Überprüfung und Zugriffskontrolle durchgesetzt werden.

Der ausgehende Traffic wird dann an sein vorgesehenes Ziel weitergeleitet, sei es das Internet, SaaS-Anwendungen oder andere Workloads und Server, die in anderen öffentlichen Clouds oder Rechenzentren gehostet werden.

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

Konsistenter, umfassender Bedrohungsschutz und Data Protection

Einheitliche Richtliniendurchsetzung in allen Umgebungen

- TLS-Überprüfung und Bedrohungsschutz im Cloud-Maßstab zur Abwehr von Zero-Day-Angriffen
- DNS-Überprüfung und Inline-Data Protection zur Verhinderung von Datenverlusten
- Strenge Kontrollen zur Einschränkung der Verbindungsziele für Workloads und Server

Reduziert die Angriffsfläche und verhindert die laterale Verbreitung von Bedrohungen

Verbindung von Anwendungen statt Netzwerken

- Zugriff nach dem Prinzip der minimalen Rechtevergabe, um Workloads mithilfe von IP, FQDN, VPC, VNet oder Tags zu segmentieren
- Eliminierung der Angriffsfläche im Netzwerk durch Verbindung von Workloads über die Zero Trust Exchange
- Unterstützung für Verbindungen von Cloud zu Cloud, Cloud zu Rechenzentrum, Region zu Region

Geringere Komplexität und Kosten

Eine Cloud-Plattform zum Schutz aller Workloads

- Sichern Sie Workloads aller großen Cloud-Service-Provider, einschließlich AWS, Azure und GCP, mithilfe einer einheitlichen Plattform.
- Automatisieren Sie Sicherheitsbereitstellungen durch programmierbare Schnittstellen mithilfe von Infrastructure-as-Code-Vorlagen (IaC).
- Nutzen Sie Integrationen von Public Cloud Service Providern wie AWS Gateway Load Balancer, userdefinierte AWS-Tags und AWS Auto Scaling

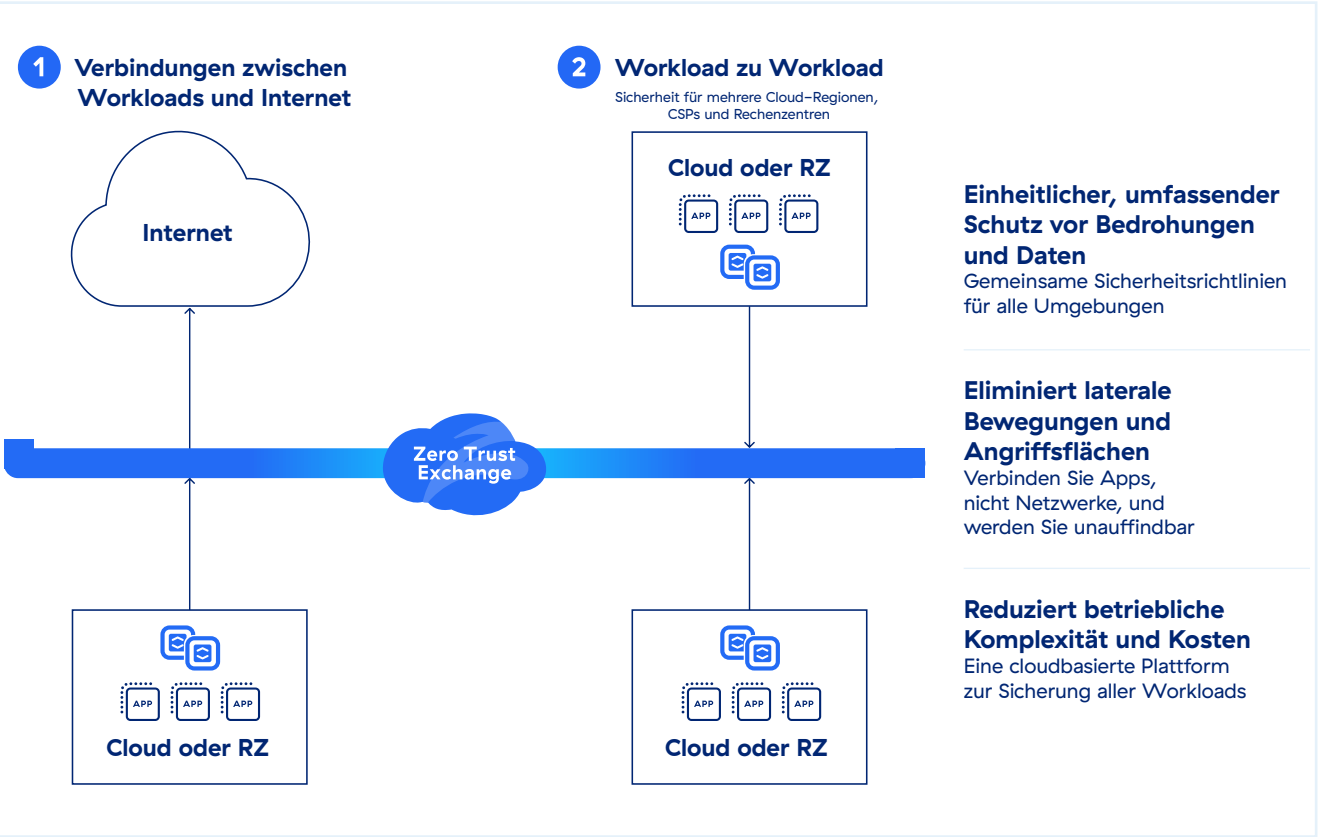


ABBILDUNG Zscaler Zero Trust für Workloads

Leistungsumfang von Zero Trust Cloud

Zero Trust Cloud basiert auf der Zero Trust Exchange von Zscaler, die User, Geräte und Anwendungen unter Verwendung von Unternehmensrichtlinien über jedes Netzwerk und jede Cloud sicher und in großem Umfang miteinander verbindet.

Zero Trust Proxy-Architektur: Speziell entwickelte, mandantenfähige Proxy-Architektur, die Quellen und Ziele sicher verbindet und gleichzeitig vollständige Transparenz des ausgehenden Datenverkehrs bietet.

TLS-Entschlüsselung im Cloud-Maßstab: Die leistungsfähige Prüfung erfolgt durch eine auf Skalierbarkeit ausgelegte Single-Scan-Multi-Access-Architektur.

Granulare App-zu-App-Segmentierung: Zero-Trust-Zugriff nach dem Prinzip der minimalen Rechtevergabe für alle Workloads und Server vereinfacht die Durchsetzung und Verwaltung von Unternehmensrichtlinien.

Bidirektionale Bedrohungsüberprüfung: KI-gestützter Bedrohungsschutz — unterstützt durch 500 Billionen tägliche Signale und 320 Milliarden tägliche Transaktionen — gewährleistet stets verfügbaren, hochgradig zuverlässigen Schutz vor Ransomware, Zero-Day-Bedrohungen und unbekannter Malware.

Inline Data Protection: Leistungsstarke, skalierbare DLP-Prüfung für alle Kanäle und Standorte.

Integrierte Multi-Cloud-fähige Plattform: Eine einheitliche Plattform bietet Richtlinienverwaltung, Traffic-Überwachung und Protokollverfolgung. Standardisierte Richtlinien werden in AWS, Azure, GCP und lokalen Rechenzentren angewendet.

Funktionsumfang von Zero Trust Cloud

ZSCALER ZERO TRUST CLOUD PLATFORM	
FUNKTION	**DETAILS**
Zuverlässiger Schutz für öffentliche Cloud-Umgebungen und On-Premise-Umgebungen	Unterstützt die Sicherung von Workloads in AWS, Microsoft Azure, Google Cloud Platform, Microsoft Azure China-Regionen und AWS GovCloud mit zusätzlicher Unterstützung für lokale Rechenzentrumsserver. FedRamp-zertifiziert für AWS GovCloud.
TLS/SSL-Überprüfung	TLS/SSL-Traffic wird lückenlos überprüft, um Bedrohungen und Datenverluste im verschlüsselten Traffic zu erkennen. Basierend auf Datenschutzanforderungen oder behördlichen Auflagen kann angegeben werden, welche Webkategorien oder Anwendungen geprüft werden sollen.
Protokoll-Streaming	Konsolidieren Sie mit dem Zscaler Nanolog Streaming Service Protokolle aller Workloads und Server weltweit in einem unternehmensspezifischen zentralen Repository. Administratoren können Transaktionsdaten von Cloud-Workloads in Echtzeit anzeigen und auswerten.
Infrastruktur als Code	Zscaler bietet Terraform-Vorlagen und -Anbieter, die die Bereitstellung und Implementierung von Sicherheitsrichtlinien und virtuellen Cloud-Connector-Maschinen automatisieren.
Konnektivitätsunterstützung	Nutzen Sie IPsec, GRE oder Cloud Connectors, um den ausgehenden Workload-Datenverkehr zur Zero Trust Exchange zu leiten. IPsec und GRE sichern den Traffic von der Workload zum Internet. Cloud Connectors werden verwendet, um sowohl den Internet- als auch den Workload-Traffic zu sichern.

ZSCALER INTERNET ACCESS FÜR WORKLOAD-TO-INTERNET	
FUNKTION	**DETAILS**
Kommunikation zwischen Workloads und Internet Schutz	Verhindern Sie Cyberbedrohungen und Datenverluste bei der Kommunikation zwischen Workloads und Internet. SSL-Überprüfung, IPS, URL-Filterung und Data Protection für die gesamte Kommunikation sind im Funktionsumfang inbegriffen.
URL-Filtering	Der User-Zugriff kann für bestimmte Webkategorien oder -ziele zugelassen, blockiert, mit Warnmeldungen versehen oder eingeschränkt werden, um webbasierte Bedrohungen zu verhindern und die Einhaltung von Unternehmensrichtlinien zu gewährleisten.
Advanced Threat Protection Schutz	Komplexe Cyberangriffe wie unter anderem Malware, Ransomware, Supply-Chain-Angriffe oder Phishing können mit proprietärer Advanced Threat Protection abgewehrt werden. Auf Grundlage der Risikotoleranz des jeweiligen Unternehmens lassen sich granulare Richtlinien festlegen.
Malware-Analyse	Unbekannte Bedrohungen, die sich in schädlichen Payloads verbergen, lassen sich zur Verhinderung von Patient-Zero-Angriffen mit fortschrittlichen KI/ML-Funktionen erkennen, abwehren und unter Quarantäne stellen.
Intrusionsschutz	Erhalten Sie vollständigen Schutz vor Bedrohungen wie Botnets, komplexen Bedrohungen und Zero-Day-Angriffen sowie kontextbezogene Informationen zu Usern, Anwendungen und Bedrohungen. Cloud- und Web-IPS lässt sich nahtlos mit Firewall, Sandbox, DLP und CASB verwenden.
DNS-Sicherheit	Identifizieren Sie verdächtige Command-and-Control-Verbindungen und leiten Sie diese zur vollständigen Inhaltsprüfung an Zscaler weiter.
DNS-Filterung	Kontrollieren und blockieren Sie DNS-Anfragen an bekannte schädliche Ziele.
Dateikontrolle	Basierend auf Workload-Identität oder Anwendung kann das Herunterladen/Hochladen von Dateien zu Anwendungen blockiert bzw. zugelassen werden.
Bandbreitenübersicht (Dashboard)	Setzen Sie Bandbreitenrichtlinien durch und priorisieren Sie geschäftskritische Anwendungen gegenüber privatem Traffic.
Dynamische, risikobasierte Zugriffs- und Sicherheitsrichtlinien	Passen Sie Sicherheits- und Zugriffsrichtlinien automatisch an Workloads, Server, Internetziele und Inhaltsrisiken an.
Korrelierte Bedrohungs-informationen Insights	Durch Kontextualisierung und Korrelation von Warnmeldungen mit Informationen zu Bedrohungseinstufung, betroffenen Ressourcen, Schweregrad usw. können Sicherheitsvorfälle schneller untersucht und behoben werden.
Inhaltsfilterung und Stateful Rules	Richtlinienbasierte Filterung in 6 Klassen, 101 Kategorien und 29 Superkategorien. Nutzen Sie die dynamische Inhaltsklassifizierung für unbekannte URLs und Safe Search. Wenden Sie detaillierte Richtlinien nach IP-Adresse, Gruppen und gehosteten Identitäten an.

ZSCALER PRIVATE ACCESS FÜR WORKLOAD-TO-WORKLOAD-TRAFFIC	
FUNKTION	**DETAILS**
Workload-zu-Workload-Segmentierung	Sichere Verbindungen und Kommunikation zwischen Workloads in Hybrid- und Multicloud-Umgebungen.
Anwendungserkennung	Automatische Erkennung und Katalogisierung von Anwendungen mithilfe bestimmter Domainnamen und IP-Subnetze für detaillierte Einblicke in den Status privater Anwendungen sowie der potenziellen Angriffsfläche.
KI-gestützte App-Segmentierung	ZPA liefert automatisch ML-basierte Empfehlungen zur Unterstützung einer effektiven Anwendungssegmentierung und Erstellung entsprechender Zugriffsrichtlinien. Die ML-gestützte Segmentierung basiert auf maschinellen Lernmodellen, die kontinuierlich anhand von Millionen Kundensignalen und Zugriffsmustern von Anwendungen trainiert werden, und ermöglicht somit eine beträchtliche Verkleinerung der internen Angriffsfläche.
Anwendungsschutz	Schützen Sie private Unternehmensanwendungen und Infrastrukturen vor allen gängigen Angriffen mit einer leistungsstarken Inline-Sicherheitsprüfung der gesamten Anwendungs-Payload zur Erkennung von Bedrohungen. Erkennen und blockieren Sie bekannte Web-Sicherheitsrisiken wie die OWASP Top 10 und neu auftretende Zero-Day-Schwachstellen, die herkömmliche Netzwerksicherheitskontrollen umgehen können.

DATA PROTECTION	
FUNKTION	**DETAILS**
Inline Data Protection (Datenübertragung)	Mithilfe von Weiterleitungsproxy und SSL-Überprüfung können Unternehmen in Echtzeit kontrollieren, ob vertrauliche Informationen an riskante Webziele oder cloudbasierte Anwendungen übertragen werden. So lassen sich interne und externe Bedrohungen der Datensicherheit beheben. Erweiterter Inline-Schutz wird für genehmigte und inoffiziell genutzte Anwendungen gleichermaßen bereitgestellt. Netzwerkgeräteprotokolle sind dazu nicht erforderlich.
Exact Data Match (EDM)	Fingerabdruck und sichere individuelle Unternehmensdaten.
Indexed Document Match (IDM)	Erstellen Sie Fingerabdrücke und sichern Sie userdefinierte Dokumente und Formulare.
Optical Character Recognition (OCR)	Erkennen und verhindern Sie Datenverluste in Bildern und Screenshots.

(Die aufgeführten Funktionen sind nicht in allen Lizenzen inbegriffen. Bestimmte Leistungen und Funktionen sind möglicherweise nur mit verschiedenen Zscaler-Editionen verfügbar.)

ZSCALER ZERO TRUST CLOUD EDITIONEN	
EDITION	**FUNKTIONEN**
Zero Trust für Workloads Standard	• Jahresabonnement für 1 GB monatlichen Datenverkehr für Zero Trust for Workloads Standard: • Beinhaltet Stateful Filtering und Cloud Connector
Zero Trust für Workloads Advanced	• Funktionsumfang der Workloads Standard Edition • Internet Access für Workloads: SSL/TLS-Überprüfung, Advanced Threat Protection, Cloud NSS, Source IP Anchoring • Private Access für Workloads: App Segments, Sub-Location, LSS Standard Logging und Reporting • Data Protection für Workloads: Inline-Web (nur im Überwachungsmodus) • Cyber Protection für Workloads: Standard-Firewall, DNS-Kontrolle
Zero Trust für Workloads: Advanced Plus	• Funktionsumfang der Workloads Advanced Edition • Data Protection für Workloads: Inline Data Protection und erweiterte Klassifizierung • Cyber Protection für Workloads: Firewall Advanced für Workloads, Sandbox Advanced für Workloads

zscaler™ | Experience your world, secured.™

Über Zscaler
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, zuverlässiger und sicherer arbeiten können. Die Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an beliebigen Standorten vor Cyberangriffen und Datenverlust. Die SSE-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