DATENBLATT

Zero Trust Device Segmentation

Vereinfachter Schutz vor lateralen Bedrohungen für Zweigstellen-, Fabrik- und Campusnetzwerke

Die Gerätesegmentierung ist ein wesentlicher Bestandteil von Zscaler Zero Trust Networking und hilft IT-Teams, Risiken zu reduzieren, die Compliance zu verbessern und die Betriebszeit zu erhöhen, indem Ursachen für laterale Bedrohungsbewegungen in Unternehmensnetzwerken beseitigt werden.

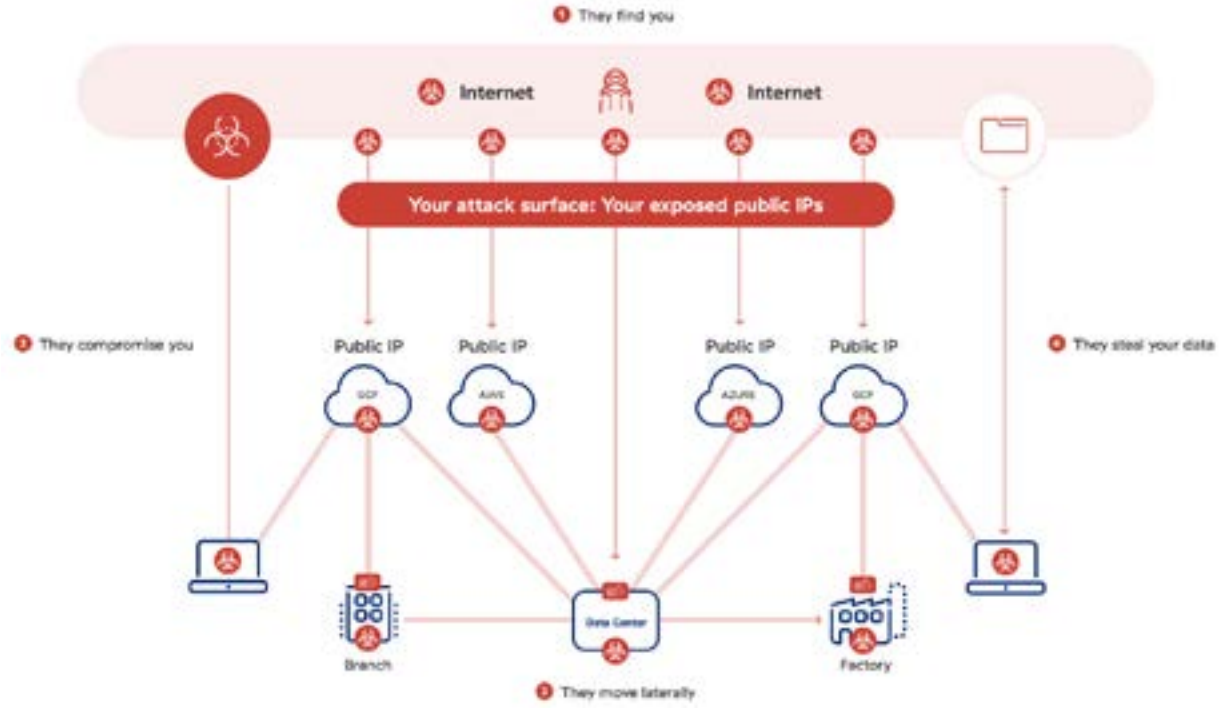
Eine sich ständig weiterentwickelnde Bedrohungs- und Compliance-Landschaft

In letzter Zeit ist es zu einem Anstieg der Warnmeldungen und Warnungen vor Cyberangriffen staatlich geförderter Bedrohungsakteure auf die kritische Infrastruktur der USA gekommen. Am 7. Februar 2024 veröffentlichten das Federal Bureau of Investigation (FBI) und die Cybersecurity and Infrastructure Security Agency (CISA) zusammen mit der National Security Agency eine Warnung an Regierungsbehörden, dass Cyber-Akteure im Begriff seien, kritische Infrastrukturen wie Transportsysteme, Öl- und Erdgaspipelines, Wasseraufbereitungsanlagen und Stromnetze zu stören. Dies ergänzt ähnliche Maßnahmen der TSA zur Sicherung von Flughäfen, Flugzeugbetreibern und Eisenbahnen, die jüngsten Cybersicherheits-Grundlinien des Energieministeriums und das nahezu endgültige NERC-Update zu CIP-015-1.

Bei der Entwicklung von OT-/IoT-Technologien steht Geschwindigkeit und Transaktionseffizienz im Vordergrund, während Sicherheit nur eine Nebenrolle spielt. Leider ist OT/IoT mittlerweile ein beliebtes Ziel von Cyberkriminellen. Laut Untersuchungen von Zscaler ThreatLabz ist die Zahl der Angriffe dort im Vergleich zum Vorjahr um 400 % gestiegen. Ransomware ist die beliebteste Angriffsstrategie und 61 % aller Sicherheitsverletzungen zielten auf Unternehmen mit vernetzter OT ab.

Zscaler Zero Trust Networking

Eine einfachere, sicherere und kostengünstigere Kommunikationsmöglichkeit für User, Geräte und Workloads



So kommt es zu Ransomware–Angriffen

EPA, CISA und FBI empfehlen den Systembetreibern dringend, entsprechend der Durchführungsverordnung des Präsidenten auf Zero Trust als Richtlinie für eine bessere Cybersicherheit umzusteigen. Die hervorgehobenen Elemente sind Schlüsselbereiche in diesen Empfehlungen, in denen Zscaler mit Zero–Trust–basierten Lösung zur Gerätesegmentierung sofort helfen kann.

- Weniger Exposition gegenüber dem öffentlichen Internet
- Geringeres Risiko von Schwachstellen
- Netzwerksegmentierung
- Protokollierung
- Keine Verbindungen unbefugter User
- Keine ausnutzbaren Dienste im Internet
- Eingeschränkte OT/IoT–Verbindungen zum Internet
- Erkennen relevanter Bedrohungen
- Bestandsaufnahme von OT–/IT–Ressourcen

Eine sicherere Architektur für die Gerätesegmentierung

Segmentierung ist seit langem ein fester Bestandteil der Netzwerktechnik, wobei Tools wie Zugriffskontrolllisten (ACLs) und Firewalls den Traffic zwischen Client und Server verwalten. Die OT–Segmentierung verlagert den Fokus jedoch auf den anfälligeren lateralen Traffic zwischen Geräten und Workloads. Aufgrund der veralteten Switching–Architektur können Geräte in gemeinsam genutzten VLANs alle anderen Geräte sehen und mit ihnen kommunizieren. Dadurch entsteht eine Umgebung, in der sich Malware leicht verbreiten kann. Leider können agentbasierte Lösungen, die für Cloud–Workloads entwickelt wurden, die in der OT so häufig vorkommenden Legacy– und Headless–Maschinen nicht segmentieren, und herkömmliche ACL–basierte Ansätze sind weiterhin mit hohem Aufwand verbunden.

Dashboard der Zero Trust Device Segmentation

Zscaler hat Zero Trust Networking als einfachere, sicherere und kostengünstigere Möglichkeit für die Kommunikation zwischen Usern, Geräten und Workloads eingeführt. Die Gerätesegmentierung ist ein zentraler Bestandteil dieses Ansatzes und ein grundlegender Schritt zur Schaffung granularer Transparenz und Kontrolle für das moderne Netzwerk.

Zscaler beseitigt die Probleme der Intra-VLAN-Segmentierung mit einer agentenlosen Lösung, die alle lateralen Bedrohungen stoppt, indem sie jedes IP-Endgerät, einschließlich Legacy- und Headless-Systeme, in einem einzelnen Netzwerksegment isoliert. Dadurch werden komplexe ACLs überflüssig und es sind keine Änderungen an der vorhandenen Infrastruktur erforderlich. Gleichzeitig wird eine hochgradig granulare und effektive Segmentierung bereitgestellt, die derzeit unübertroffen ist.

Anwendungsfälle

Zu den häufigsten Anwendungsfällen für die agentenlose Gerätesegmentierung gehören:

LAN-interne Segmentierung
Erweitern Sie Zero Trust auf das LAN, indem Sie die Segmentierung des East-West-Traffics erzwingen. Dies verkleinert Ihre interne Angriffsfläche und eliminiert die Gefahr von lateralen Bewegungen in kritischen OT-/IoT-Netzwerken, ohne dass eine NAC- oder Firewall-basierte Segmentierung erforderlich ist.

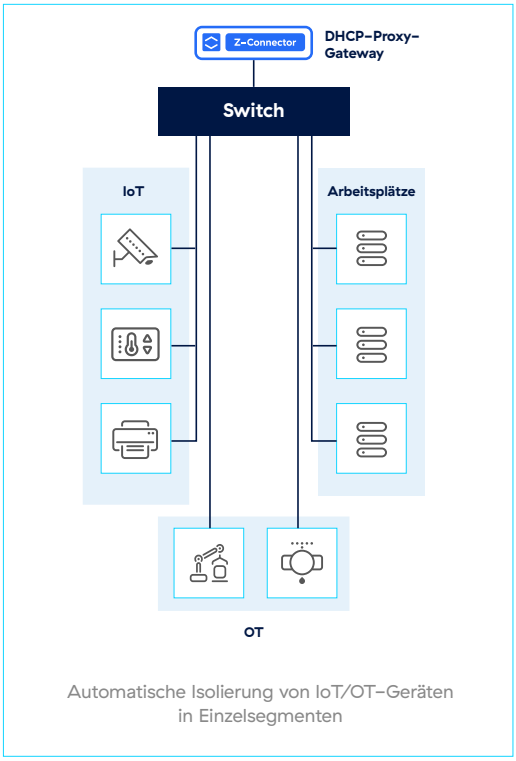
So setzen Sie Zero-Trust-Segmentierung in Ihrem Netzwerk durch:

- Isolieren Sie jedes Geräts in einem Einzelsegment (/32).
- Gruppieren Sie Geräte, User und Anwendungen automatisch, indem Sie ihre Trafficmuster analysieren. So verhindern Sie, dass betrügerische Geräte mithilfe von MAC-Spoofing in das Netzwerk gelangen.
- Setzen Sie Richtlinien für East-West-Traffic basierend auf der Identität und dem Kontext von Usern und Geräten dynamisch durch.

IT-/OT-Segmentierung

Zscaler Zero Trust Device Segmentation fungiert als Kill Switch für Ransomware und deaktiviert nicht unbedingt erforderliche Gerätekommunikation, um die laterale Ausbreitung von Bedrohungen zu stoppen, ohne den Geschäftsbetrieb zu unterbrechen. Diese Lösung neutralisiert fortgeschrittene Bedrohungen wie Ransomware auf IoT-Geräten, OT-Systemen und agentenlosen Geräten.

- Gruppieren Sie bekannte MAC-Adressen auf allen Geräten autonom und setzen Sie entsprechende Richtlinien durch (z. B. wird der RDP-Zugriff auf Kameras außer für Administratoren verweigert).
- Automatische Isolierung unbekannter MAC-Adressen, um das Schadenspotenzial im Falle eines kompromittierten Geräts zu begrenzen
- Integration mit Asset-Management-Systemen für sichere Zugriffskontrollrichtlinien



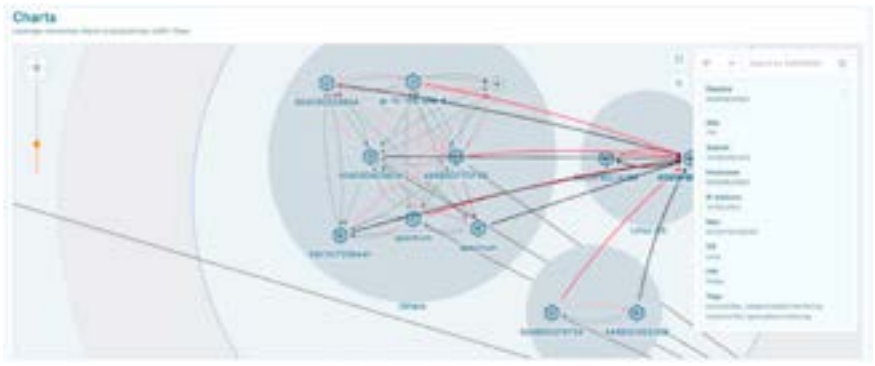
Automatische Isolierung von IoT/OT-Geräten in Einzelsegmenten

Automatische Geräteerkennung und -klassifizierung

Da ein erheblicher Anteil des OT/IoT-Traffic innerhalb des lokalen Netzwerks bleibt, ist eine kontinuierliche Sichtbarkeit des lateralen Traffics wichtig. Durch die automatische Geräteerkennung und -klassifizierung können Netzwerkadministratoren Leistung, Verfügbarkeit und Sicherheit für IoT/OT-Systeme ohne komplexe Bestandsverwaltung besser verwalten.

Für Netzwerk- und Gerätesichtbarkeit:

- Entdecken, klassifizieren und inventarisieren Sie OT/IoT-Geräte ohne Installation von Endgerät-Agenten
- Erhalten Sie eine Baseline der Trafficmuster und des Geräteverhaltens, um befugte und nicht befugte Zugriffe zu ermitteln
- Gewinnen Sie präzise Netzwerkeinblicke für das Leistungsmanagement und die Bedrohungsverfolgung

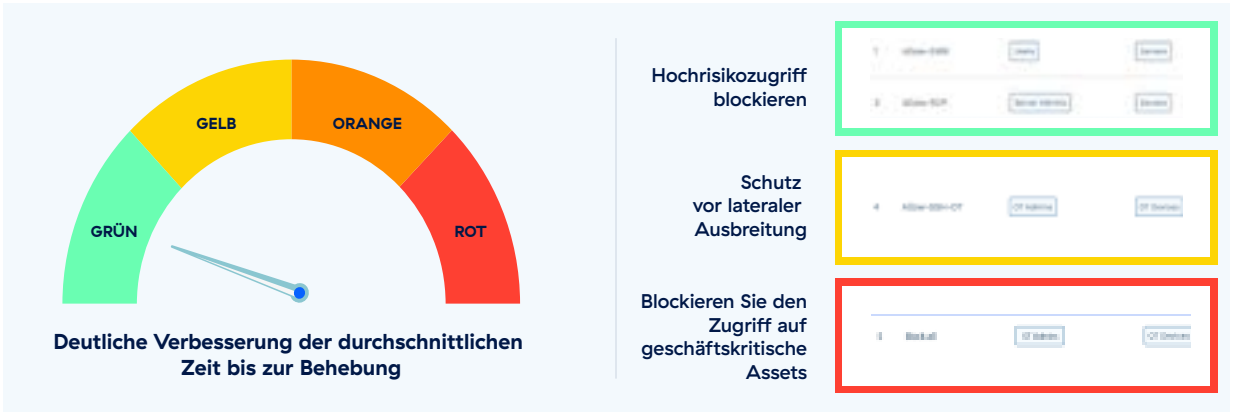


Dashboard Device Discovery

Automatisierte Reaktion auf Vorfälle

Wir stellen den Zscaler Ransomware Kill Switch vor. Die Reduzierung der Angriffsfläche mit einem Klick ist vollständig in unsere Zero-Trust-Device-Segmentation-Lösung integriert. Sperren Sie bekannte anfällige Protokolle und Ports und deaktivieren Sie sogar sofort den Zugriff auf kritische Netzwerke wie ganze Krankenhäuser oder Fabrikhallen. Und das alles mit voreingestellten Schweregraden, um Ausfallzeiten im Unternehmen zu minimieren.

Der Ransomware Kill Switch fungiert als mehrschichtiger Durchsetzungspunkt für Richtlinien und ermöglicht abgestufte Reaktionen auf Vorfälle bei einer aktiven Kompromittierung sowie eine Erweiterung der bestehenden Investitionen in Sicherheitstools. Jede Ebene des Ransomware Kill Switch verfügt über Funktionen, die „virtuellen Sicherungen" oder Defcon-Ebenen ähneln, mit vordefinierten Eskalationspfaden, um die gesamte unnötige Netzwerkkommunikation zu oder von einem Endgerät zu blockieren, eine laterale Ausbreitung zu verhindern und die Angriffsfläche drastisch zu reduzieren.



Diese Lösung deaktiviert sofort jegliche nicht notwendige Gerätekommunikation, um die laterale Ausbreitung von Bedrohungen zu stoppen, ohne den Geschäftsbetrieb zu unterbrechen. Diese Lösung neutralisiert fortgeschrittene Bedrohungen wie Ransomware auf IoT-Geräten, OT-Systemen und agentenlosen Geräten.

Zscaler bietet die vollständige Kontrolle über den Ransomware Kill Switch über APIs. Mithilfe dieser programmierbaren Schnittstellen können IT-Unternehmen vorhandene Sicherheitsorchestrierungstools wie SIEM- (Security Information and Event Management), SOAR- (Security Orchestration and Response) oder EDR/XDR-Lösungen aktivieren, um die Reaktion auf Vorfälle zu automatisieren, kompromittierte Endgeräte sofort unter Quarantäne zu stellen und den Infektionsradius einzudämmen.

So erhalten Unternehmen Investitionsschutz für ihr bestehendes Netzwerk und ihre Sicherheitsinfrastruktur und verbessern gleichzeitig sofort den Sicherheitsstatus des Unternehmens.

Geschäftsnutzen

Granulare Eindämmung zur Begrenzung der lateralen Ausbreitung

Vorab geplante, automatisierte Reaktion auf Vorfälle beim Eintreten einer Datenpanne

Strikte Eindämmung an wichtigen Grenzschichten, z. B. zwischen der Unternehmens-IT und den zentralen Netzwerken

Ordnungsgemäße Abschaltung verdächtiger Ports und Protokolle zur Maximierung der Betriebszeit

Unterbinden Sie laterale Bedrohungsbewegungen im LAN:
Minimieren Sie die Angriffsfläche, indem Sie jedes Gerät in einem separaten Netzwerk isolieren, wodurch die Angriffsfläche und das Risiko der Ausbreitung von Bedrohungen beseitigt werden. Selbst kompromittierte Geräte können andere Geräte nicht mehr infizieren.

Reduzieren Sie die Komplexität und die Kosten, die mit Legacy-Segmentierungstools einhergehen:
Segmentieren Sie jedes IP-Endgerät ohne die Komplexität veralteter, IP-zentrierter Netzwerktechnologien wie NAC und East-West-Firewalls oder komplexer Konstrukte wie ACLs und manueller VLAN-Segmentierung.

Verschaffen Sie sich einen besseren Überblick über den East-West-Traffic:
Mit der automatischen Geräteerkennung und -klassifizierung erhalten Netzwerkadministratoren vollständige laterale Transparenz und können die Performance, Verfügbarkeit und Sicherheit jedes Geräts besser verwalten, selbst bei solchen, auf denen keine Agents ausgeführt werden können.

Bereitstellung ohne Netzwerkunterbrechung:
Profitieren Sie von agentenloser Technologie, die sich schnell bereitstellen lässt, ohne die aktuelle Arbeitsweise des Kunden zu stören, und keine Änderung der Netzwerkarchitektur oder eine neue IP-Adressierung der Geräte erfordert.

Schnellere Compliance:
In den branchenübergreifenden Cybersicherheitsstandards der Regierung wird die Segmentierung nun als Eckpfeiler von Zero Trust genannt. Der agentenlose Ansatz von Zscaler lässt sich schnell bereitstellen und verbessert die Compliance sofort.

Funktionen

Isolierung durch Airgaps

- Isolierung von Geräten ohne Agent
- Gerätequarantäne mit einem Klick
- Erkennung von Verstößen gegen die Airgap-Isolierung
- MAC-adressbasierte Filterung

Zero-Trust-Segmentierung

- Netzwerkbasierte Segmentierung

Gerätebasierte Segmentierung

- Autonome Gruppierung und Richtlinien
- IntraVLAN- und InterVLAN-Richtliniensteuerung
- Dynamische tagbasierte Richtlinien
- Richtlinien auf Grundlage von Geräte- und Useridentität
- Zeitbasierte Richtlinien
- Zonenbasierte Richtlinien
- Hierarchisches Richtlinienframework

Identifizierung und Profilerstellung von Ressourcen

- Endgeräte- und Netzwerkerkennung
- Fingerprinting von Geräten
- Profilbasierte Gerätekategorisierung
- Entschlüsselung von ICS-/medizinischen Protokollen

Hohe Verfügbarkeit

- Zwei-Knoten-Cluster mit VRRP
- VRRP mit Sitzungssynchronisierung
- Konfigurations- und Statussynchronisierung
- Link-Aggregation
- Überwachung der Schnittstellenaktivität
- Unterbrechungsfreie Software-Upgrades
- Hardwareaustausch im Betrieb

Routing- und Netzwerkservices

- Dynamisches Routing — BGP, OSPF
- Multicast-Routing — IGMP, PIM
- DHCP-Server, Relay/Proxy
- VLAN-Trunking
- Netzwerkadressübersetzung
- Richtlinienbasiertes Routing
- Equal Cost Multi Path (ECMP)
- Standort-zu-Standort VPN

Reaktion auf Vorfälle

- Ransomware Kill Switch

Transparenz und Protokollierung

- Traffic-Mapping mit Richtlinienkorrelation
- Integrierter Elastic Data Lake
- Session-init-Protokolle für jegliche Kommunikation innerhalb von und zwischen Segmenten
- Protokollexport zu SIEM/Log Collector

Flexible Bereitstellungsmodelle

- Zero-Touch-Bereitstellung des Airgap-Gateways
- Vorlagen und Profile für Standorte
- Standalone-, Hochverfügbarkeitscluster- oder Multicluster-Bereitstellung
- Physische oder VM-basierte Airgap-Gateways

Monitoring und Fehlerbehebung

- Remote-Debug-Konsole
- Lokales CLI auf Airgap-Gateways
- SNMP-Unterstützung

Zentralisiertes cloudbasiertes Management

- Single Sign-On (SSO) und MFA
- Audit Trails für Anmeldeereignisse und Konfigurationsänderungen
- Rollenbasierte Zugriffskontrolle
- Mandantenfähige, über die Cloud bereitgestellte Plattform
- API-basierter Zugriff

Integrationen von Drittanbietern

- Microsoft Active Directory
- SIEM-Integration
- EDR-Anbieter — Crowdstrike, SentinelOne
- Ressourcenverwaltung — Armis
- SSE — Zscaler ZIA

Dimensionierung der Zscaler-Gateway-Appliance

Im Folgenden finden Sie verschiedene Größenangaben für physische oder virtualisierte Zscaler-Gateway-Appliances.

Hardwarespezifikationen für die Bereitstellung physischer Gateways						
	XS	S1	S2	M	L	XL
Verfügbarkeit	Juni 2024	Juni 2024	jetzt	jetzt	jetzt	1Q GJ25
Hardwaremodell	ZT 400	ZT 600	Dell VEP4600	Dell VEP4600	Dell VEP4600	N. N.
CPU	4C Atom	8C Atom	4C Xeon	8C Xeon	16C Xeon	16C Xeon
Speicher	16 GB	16 GB	16 GB	32 GB	64 GB	64 GB
Storage	64 GB	64 GB	128 GB	256 GB	960 GB	256 GB
Ports	4x 1 GbE	4x 1 GbE	6x 1GbE 2x 1GbE (SFP)	4x 1 GbE 2x 10 GbE	4x 1 GbE 6x 10 GbE	4x 25 GbE
Formfaktor	Desktop	Desktop	1U	1U	1U	1U
Andere Merkmale	Ohne Lüfter		RPS	RPS	RPS	RPS
Durchsatz (64 KB HTTP)	4 Gbit/s	8 Gbit/s	10 Gbit/s	20 Gbit/s	40 Gbit/s	80 Gbit/s
Sessions	250.000	500.000	500.000	1 Mio.	2 Mio.	2 Mio.
Anzahl Endgeräte	200	500	1,000	2.000	4.000	N. N.

Größenleitfaden für virtuelle Appliances				
	XS	S1	S2	M
Verfügbarkeit	jetzt	jetzt	jetzt	jetzt
CPU	2 vCPU	4 vCPU	8 vCPU	16 vCPU
Speicher	8 GB	16 GB	32 GB	64 GB
Storage	256 GB	256 GB	256 GB	256 GB
Ports	4x vNICs	4x vNICs	4x vNICs	4x vNICs
Durchsatz (64 KB HTTP)	5 Gbit/s	10 Gbit/s	20 Gbit/s	40 Gbit/s
Sessions	250.000	500.000	1 Mio.	2 Mio.
Anzahl Endgeräte	200	500	2.000	4.000

Mit einem technischen Experten sprechen

Möchten Sie mehr darüber erfahren, wie Zscaler zum Schutz der kritischen Infrastruktur Ihres Unternehmens beitragen kann? Vereinbaren Sie einen Termin für ein Gespräch mit einem unserer technischen Experten.

zscaler™ | Experience your world, secured.™

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 Datenverlust. Die SASE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und ist 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