Zscaler Zero Trust SD-WAN

Verbinden Sie Zweigstellen, Fabriken und Rechenzentren sicher, ohne geroutete Overlays oder laterale Bedrohungsbewegungen.

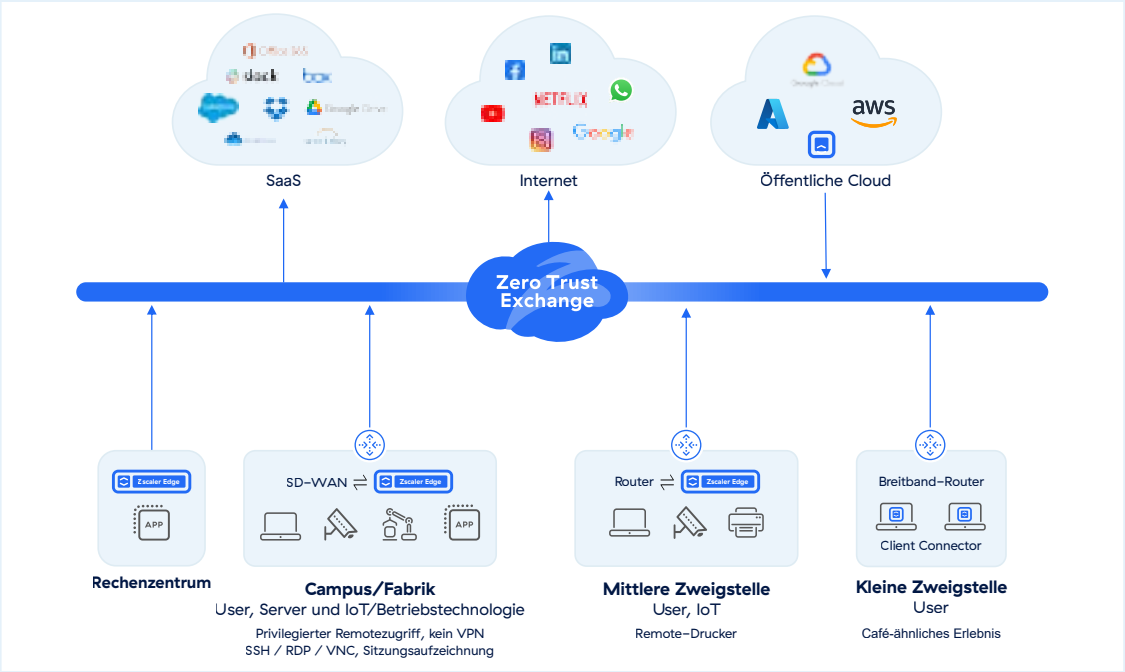
Herkömmliche SD-WANs erweitern Ihr Netzwerk auf Remote-Zweigstellen und in die Cloud. Dadurch wird Ihre Angriffsfläche vergrößert, Bedrohungen können sich seitlich ausbreiten und Ransomware-Angriffe werden erleichtert.

Die Sicherung herkömmlicher Netzwerke erfordert einen komplexen Flickenteppich aus Firewalls, Proxys, NAC-Gateways und Endpunkt-Agenten, was zu einem unkontrollierten Anstieg von Kosten und Komplexität führt. Letztendlich sind Sie weiterhin angreifbar, da Umfang und Häufigkeit von Ransomware-Angriffen immer weiter zunehmen.

Zscaler Zero Trust SD-WAN bietet eine einfachere, sicherere und kostengünstigere Möglichkeit zur Kommunikation zwischen Usern, Geräten und Workloads, ohne die Komplexität und Sicherheitsherausforderungen gerouteter Overlay-Netzwerke.

Zscaler Zero Trust SD-WAN:

- Ermöglicht die Anbindung von Filialen, ohne Ihr Netzwerk überall auszuweiten
- Reduziert das Ransomware-Risiko durch die Eliminierung der lateralen Ausbreitung von Bedrohungen
- Verkleinert die Angriffsfläche durch Verzicht auf exponierte VPN-Ports und Firewalls
- Reduziert die Infrastrukturkosten durch radikale Vereinfachung Ihrer Netzwerkarchitektur
- Verbessert die Anwendungsleistung durch Vermeidung des Datenverkehrs-Backhauls zu Rechenzentren
- Gewährleistet Schutz vor Cyberbedrohungen sowie Data Protection durch Überprüfung des gesamten Traffics



Herkömmliche SD-WANs erleichtern Ransomware-Angriffe

Wenn Unternehmen versuchen, Zweigstellen über veraltete Netzwerk- und Sicherheitsarchitekturen mit dem Internet oder anderen Anwendungen in öffentlichen Clouds oder Rechenzentren zu verbinden, stehen sie vor einer Reihe von Herausforderungen.

- **Erweiterte Angriffsfläche:** Die Ausweitung des Netzwerks auf entfernte Zweigstellen bietet Angreifern mehr Möglichkeiten, in Ihr Unternehmen einzudringen. Jede Firewall oder jedes VPN-Gateway ist ein Einstiegspunkt, und Zero-Day-Schwachstellen sind in der Branche nach wie vor ein Problem.
- **Laterale Bedrohungsbewegung:** Ein infizierter User oder ein IoT-Gerät in einer Zweigstelle kann das Netzwerk scannen und sich lateral zu anderen Standorten, Rechenzentren und virtuellen privaten Clouds bewegen. Bei den jüngsten Ransomware-Angriffen dauerte es vom ersten Eindringen bis zu lähmenden Ausfällen nur 45 Minuten, sodass den IT-Teams keine Zeit blieb zu reagieren.
- **Kosten und Komplexität:** Der Flickenteppich aus Firewalls, Proxys, NAC-Agenten und IP-basierten Richtlinien zum Schutz und zur Segmentierung von SD-WANs erhöht die betriebliche Komplexität und die Kosten enorm und beeinträchtigt die Agilität Ihres Unternehmens.
- **Schlechte Performance und User Experience:** Das Backhauling des Traffics zu Rechenzentren und durch mehrere Sicherheitskontrollpunkte führt häufig zu einer schlechten Anwendungsleistung und einer inkonsistenten Erfahrung für die User.

Zero Trust SD-WAN unterbindet laterale Bewegungen

Zero Trust SD-WAN verbindet Ihre Zweigstellen, Fabriken und Rechenzentren sicher, ohne die Komplexität von VPNs oder Overlay-Routing. Es gewährleistet Zero-Trust-Zugriff zwischen Usern, IoT/OT-Geräten und Anwendungen basierend auf Unternehmensrichtlinien. Mit der Kombination aus der branchenführenden Zscaler Zero Trust Exchange und einer nahtlosen Konnektivität für Standorte, Clouds und User können Unternehmen ihr SASE-Framework (Secure Access Service Edge) auch auf ihre Zweigstellen ausweiten.

- Zscaler Zero Trust SD-WAN bietet Zweigstellen und Fabriken schnellen und zuverlässigen Zugriff auf das Internet sowie SaaS- und private Anwendungen mit einer Direct-to-Cloud-Architektur, die ein hohes Maß an Sicherheit gewährleistet und zudem noch einfach zu bedienen ist.
- Sie verhindert die laterale Ausbreitung von Bedrohungen und reduziert das Ransomware-Risiko für Ihr Unternehmen erheblich.
- Sie senkt die Infrastruktur- und Betriebskosten durch den Verzicht auf komplexes Routing, VPNs und Firewalls und gewährleistet gleichzeitig umfassenden Schutz vor Cyberbedrohungen sowie Data Protection.

So funktioniert Zero Trust SD-WAN

Zero Trust SD-WAN verwendet eine physische oder virtuelle Appliance, um ISP-Verbindungen von und zu Zweigstellen, Campusgeländen oder Fabriken zu verwalten und den Traffic basierend auf den Unternehmensrichtlinien an die Zero Trust Exchange weiterzuleiten. Der Traffic wird über vorübergehende DTLS-Verbindungen sicher an die Zero Trust Exchange weitergeleitet, wo er mit kontextbezogenen Sicherheitsrichtlinien auf Cyberbedrohungen und Datenverluste überprüft werden kann.

Die Zero Trust Exchange ermöglicht die bidirektionale Kommunikation zwischen Geräten und Internet-Apps oder privaten Unternehmensanwendungen, die an anderen Standorten, in Rechenzentren oder in der Cloud ausgeführt werden.

Beispielsweise kann ein Druckserver in einem Rechenzentrum Druckaufträge über die Zero Trust Exchange an einen Drucker in einer Remote-Zweigstelle senden, ohne dass hierfür geroutete Netzwerke, VPNs oder exponierte Ports erforderlich sind. Vertrauenswürdiger Anwendungstraffic kann mit direktem Internet-Breakout ohne Umwege über das Internet gesendet werden.

Dieser einzigartige Ansatz bietet drei wesentliche Vorteile:

- **Mehr Sicherheit:** Ransomware kann sich nicht lateral zwischen Standorten ausbreiten; infizierte Geräte können keine IT-Assets außerhalb ihrer lokalen Netzwerke scannen.
- **Weniger Komplexität:** Keine gerouteten Overlays, Firewalls oder Site-to-Site-VPNs mehr
- **Bessere User Experienc:** Anwendungen laufen schneller ohne Traffic-Backhauling und Sicherheitsengpässe

Anwendungsfälle für Zero Trust SD-WAN

- **Bessere Alternative zu VPN:** Eliminieren Sie die Komplexität von Site-to-Site-VPNs und gerouteten Overlays mit einer einfacheren, sichereren Zero-Trust-Lösung
- **SD-WAN-Aktualisierung:** Binden Sie Zweigstellen mit einer Zero-Trust-Architektur an und reduzieren Sie das Ransomware-Risiko
- **Fusionen** Integrieren Sie User und Apps ohne die Komplexität und Kosten der Netzwerkintegration
- **Sichere Fabriken:** Eliminieren Sie die laterale Ausbreitung von Bedrohungen zwischen Fabriken und sichern Sie IT/OT-Umgebungen

Hardware- und Softwaremodelle für Branch Connectors

Funktion	ZT 400	ZT 600	ZT 800	ZT VM
				Zscaler Edge
Typ	Kleine und mittelgroße Niederlassungen	Kleine und mittelgroße Niederlassung	Mittelgroße und große Niederlassung	Zweigstelle und Rechenzentrum
Verschlüsselter Durchsatz	200 Mbit/s	500 Mbit/s	1 Gbit/s	Variiert
Physikalische Anschlüsse	4x RJ45 GbE	6x RJ45 GbE	6x RJ45 GbE, 2x SFP	N/A
Zero-Touch-Bereitstellung	✓	✓	✓	N/A
Gateway-Modus mit App-basierter Pfadauswahl	✓	✓	✓	N/A
Granulare Weiterlei-tungsrichtlinien	✓	✓	✓	✓
Bedrohungs- und Data Protection-Richtlinien für den Internetverkehr	✓	✓	✓	✓
Sicherer privater Zugriff für IoT/OT-Geräte	✓	✓	✓	✓

TABELLE 1: VORTEILE VON ZSCALER ZERO TRUST SD-WAN	
FUNKTION	**DETAILS**
Funktionen	
Zero-Touch-Bereitstellung und automatisches Deployment	• Vorlagengestützte Zero-Touch-Provisionierung • Vollautomatische Bereitstellung • Dynamische Erkennung des geografischen Standorts von Zweigstellen
Detaillierte Weiterleitungsregeln für Internet- und Anwendungsdatenverkehr	• Optionen zum Senden des Traffics an ZIA, ZPA oder direkt (unter Umgehung der Zscaler-Services) • Flexible Traffic-Auswahlkriterien für Standort, Unterstandort, Standortgruppe, 5-Tupel oder FQDN
Einheitliche Zero-Trust-Richtlinien	• Einheitliche Regeln für den Datenverkehr zwischen Usern/IoT-Geräten und Anwendungen und zwischen verschiedenen Servern mit der erweiterten ZPA-Richtlinie zu neuen Client-Typen • Standort- und geobasierte Richtlinien • Sicherheitsrichtlinien mit IPS, SSL-Proxy, URL-Filterung und Data Protection • Kompletter Security-Stack mit vorkonfigurierter Sicherheit für IoT/OT und Server
Hohe Verfügbarkeit	• Automatisches Failover mit N+2-Redundanz sichert Servicekontinuität • Zwei Instanzen des Branch Connectors bieten zusätzliche Unterstützung für Trafficspitzen und Redundanz im Falle eines Hardwarefehlers • Ein Load Balancer ist für die aktive/passive Fehlertoleranz unter Verwendung einer virtuellen IP-Adresse (VIP) basierend auf dem Common Address Redundancy Protocol (CARP) konfiguriert.
Zentrale Übersicht und granulare Protokollierung	• Zentrale Übersicht zu Gerätezustand und Datenverkehr • Filter für Bereitstellungen in Cloud, Rechenzentren und Zweigstellen • Genaue Protokollierung sämtlicher Sitzungen und Transaktionen zu allen Ports und Protokollen einschließlich öffentlicher und privater DNS-Transaktionen • Vollständig mit der NSS-Infrastruktur integriert — vorhandene NSS-Firewall-VM kann zum Streaming der Protokolle an SIEM verwendet werden
WAN-Anschluss	• Dual-ISP-Verbindung (Ethernet) • Multihoming
LAN-Schnittstellenmanagement	• Mehrere L3-LAN-Netzwerke • 802.1q/VLAN-Tagging • DHCP-Server • DNS-Gateway
Gerätespezifische Firewall-Regeln	• Detaillierte Zugriffskontrolle für lokalen LAN-LAN-Traffic • L3-Zugriffskontrolllisten (ACL)
Anwendungsspezifische Pfadauswahl	• Dynamische Pfadauswahl für wichtige SaaS- und Privatanwendungen • Intelligente POP-Konnektivität von Zscaler • Integrierte SLA-Überwachung und Failover
Routing	• Statisches Routing
Zscaler-RZ/POP	• Die Cloud-Sicherheitsplattform von Zscaler ist auf über 150 Rechenzentren weltweit verteilt und immer nah am Kunden • Integrierte Verfügbarkeit mit nahtlosem Failover zum nächsten verfügbaren Service-POP

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