Datenblatt

Zscaler Zero Trust SD-WAN

Sichere Verbindungen für Zweigstellen, Fabriken und Rechenzentren mit ortsunabhängiger Zero-Trust-Sicherheit für Server und IoT/OT-Geräte.

Hybrides Arbeiten und die Cloud machen perimeterbasierte Netzwerk- und Sicherheitsmodelle überflüssig. Denn private Anwendungen werden zunehmend in die Cloud verlagert und der Zugriff erfolgt standort- und geräteübergreifend über das Internet.

Heute nutzen viele Unternehmen IoT/OT-Geräte an verschiedenen Standorten wie Niederlassungen, Fabriken und Rechenzentren, um ihre Abläufe zu optimieren. Und auch eine erhebliche Anzahl an Kunden verlässt sich auf die Workload-Kommunikation zwischen Server und Client. Doch herkömmliche Verfahren, die zur Steuerung des Anwendungszugriffs auf veraltete WANs, Mesh-VPNs oder Firewalls setzen, sind in der Cloud und beim mobilen Arbeiten wirkungslos.

Da sich auch die organisatorischen Anforderungen verändern, geraten die etablierten WAN-Lösungen immer mehr ins Hintertreffen. SD-WAN bringt diverse Herausforderungen mit sich, wie die geringe Sicherheit des netzwerkbasierten Zugriffs, die große Angriffsfläche, die Ausbreitung von Infektionen und das komplexe Routing. Hier Zero Trust zu gewährleisten, erfordert oft zusätzliche Firewalls, die allerdings Kosten und Komplexität weiter in die Höhe treiben.

Zscaler Zero Trust SD-WAN:

- **Standortunabhängiges Zero Trust** – für User, Geräte, Server und IoT/OT
- **Leistungsfähigere Anwendungen**, da der Datenverkehr der Zweigstellen direkt an die Zero Trust Exchange und der vertrauenswürdige Anwendungsverkehr direkt über das Internet übermittelt wird.
- **Eindämmung von Angriffen:** Zero Trust sorgt für sichere Verbindungen und ermöglicht die Segmentierung innerhalb der Netzwerkgrenzen des Unternehmens
- **Geringere Angriffsfläche** durch die Verbindung von Zweigstellen und Rechenzentren über die Zero Trust Exchange, unabhängig von der Transportschicht
- **Erkennung und Klassifizierung von Schatten-IoT** mit automatischer Geräteklassifizierung anhand von Traffic-Profilen
- **Einfacher, sicherer Zugriff auf OT-Ressourcen** durch clientlosen, browserbasierten Zugriff auf die SSH/RDP/VNC-Ports der OT-Geräte
- **Durchsetzung differenzierter Weiterleitungsrichtlinien** zum Internet- und internetexternen Datenverkehr per ZIA oder ZPA
- **Plug-and-Play-Bereitstellung:** Zero Touch Provisioning (ZTP) vereinfacht die Bereitstellung und beschleunigt die Integration

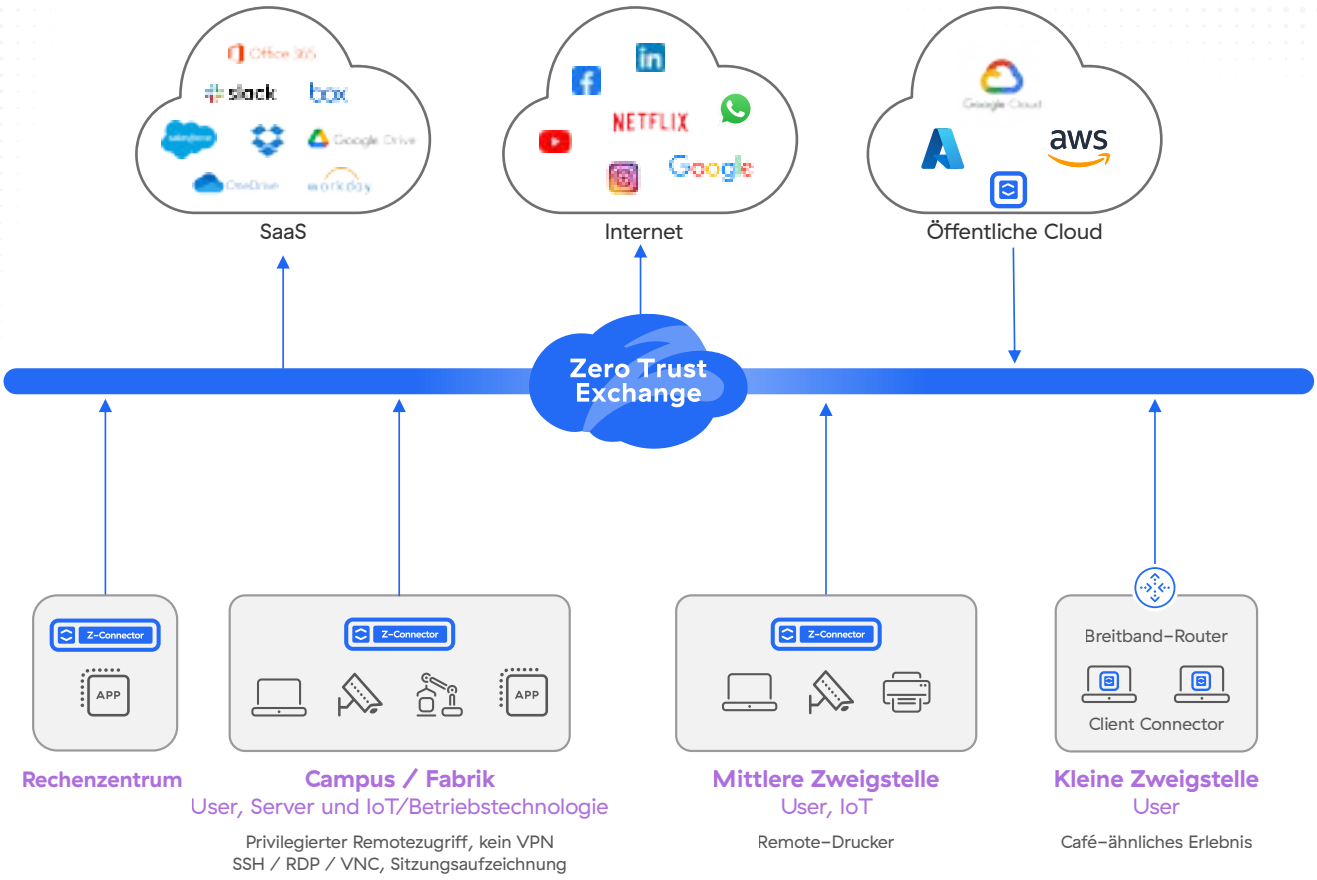

Abb. 1: Zero Trust SD-WAN

Mit Zero Trust SD-WAN verbinden Sie Niederlassungen, Fabriken und Rechenzentren sicher und ohne komplexe VPNs. So gewährleisten Sie Zero Trust für User, IoT-/OT-Geräte und Anwendungen gemäß Ihren Richtlinien.

Herkömmliches SD-WAN ist kein Zero Trust

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. Dazu zählen:

- **Erhöhtes Risiko lateraler Bewegungen und internetbasierter Angriffe** durch die Verwendung veralteter, netzwerkzentrierter Konnektivitätslösungen wie Site-to-Site-VPNs, Firewalls oder herkömmlicher SD-WANs. Diese dehnen das vertrauenswürdige Kundennetzwerk über das Internet auf andere Clouds und lokale Umgebungen aus und vergrößern so die Angriffsfläche. Der Flickenteppich aus Sicherheitsanwendungen, Tools und abweichenden Richtlinien erhöht die Gefahr durch bekannte und unerkannte Sicherheitslücken.

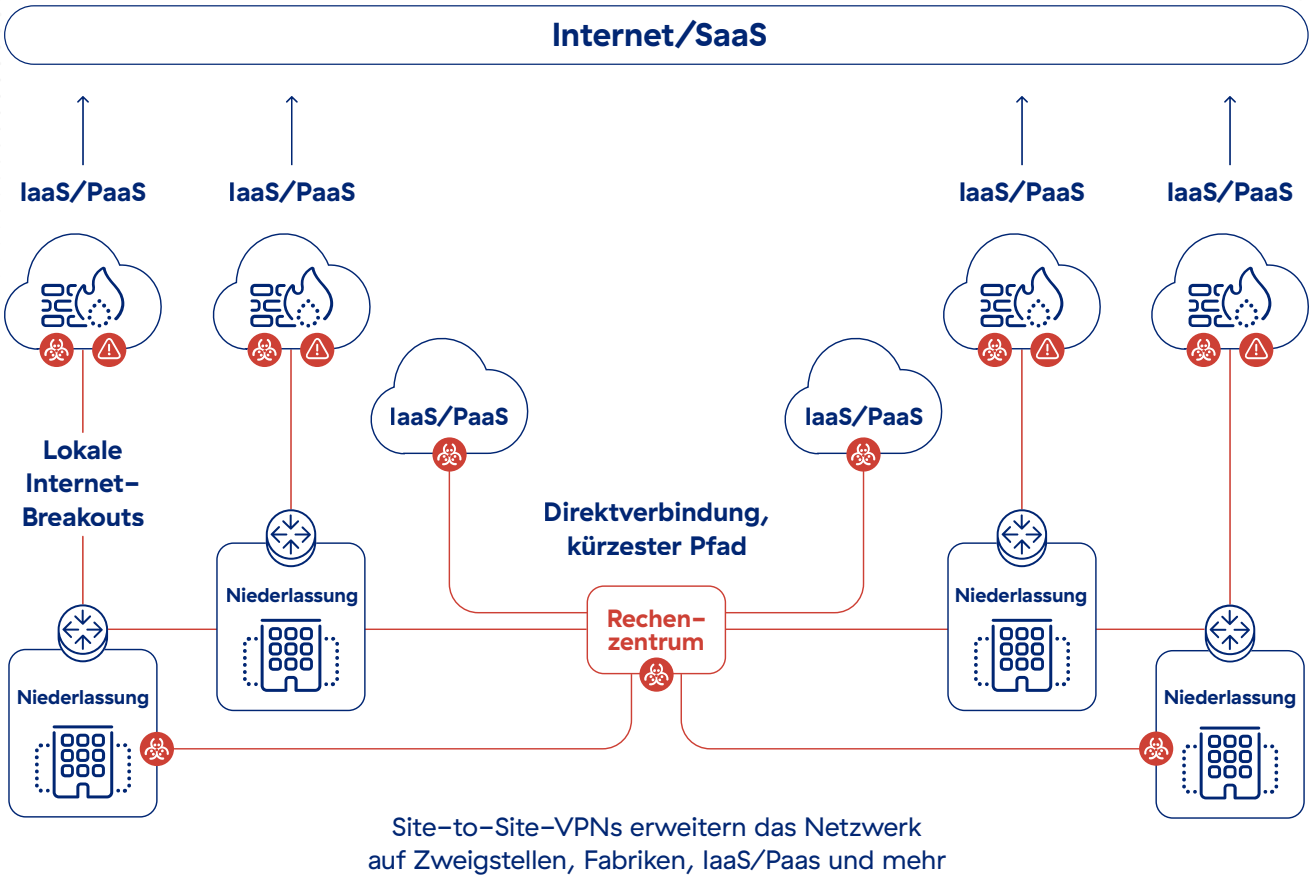

Abb. 2: Erhöhtes Risiko von Seitwärtsbewegungen und Angriffen aus dem Internet bei herkömmlichem SD-WAN

- **Mehr Komplexität** durch kompliziertes Routing, mehrere Netzwerk-Hops und -Appliances und zersplitterte Richtlinien aus der Übernahme älterer Modelle in die Cloud. Diese Komplexität stellt für Netzwerk- und Sicherheitsabteilungen eine schwierige Aufgabe dar, da Verbindungen nur schwer vereinheitlicht und Sicherheitsrichtlinien in Zweigstellen, Clouds und Rechenzentren kaum konsequent durchgesetzt werden können.
- **Mangelnde Transparenz** der Verbindungspfade von Zweigstellen, Rechenzentren und Cloud mit der Folge von Netzwerk- und Sicherheitslücken.
- **Geringe Leistung und Skalierbarkeit** wegen der wachsenden Zahl an Netzwerk- und Sicherheitsdiensten in Zweigstelle und Rechenzentrum und Engpässen bei den zentralen Sicherheitskontrollen.
- **Hohe Kosten** durch veraltete Netzwerk- und Sicherheitskomponenten (wie Firewalls, IPS, Router und andere Einzelprodukte), übermäßig viele Netzwerkdienste als Ausgleich der mangelnden Skalierbarkeit und die verstärkte Nutzung von Cloud-Diensten.

So funktioniert Zero Trust SD-WAN

Mit Zero Trust SD-WAN können Unternehmen kompakte Zweigstellen errichten und dazu Produkte wie Router, Firewalls und VPNs durch ein einfaches Plug-and-Play-Gerät ersetzen, das schnell und ausschließlich per Internetverbindung bereitgestellt wird. So können sie ihren Verwaltungsaufwand verringern und die Funktionalität insgesamt erhöhen. Zero Trust SD-WAN vereinfacht die Zweigstellenkommunikation mit einem Zero-Trust-Netzwerk-Overlay, das flexible Weiterleitung und einfache Richtlinienverwaltung mit dem bewährten ZIA- und ZPA-Framework gewährleistet.

Der Zweigstellen-Traffic wird direkt an die Zero Trust Exchange weitergeleitet, wo entweder ZIA- oder ZPA-Richtlinien für eine vollständige Sicherheitsüberprüfung und identitätsbasierte Kontrolle der Zweigstellen- und RZ-Kommunikation angewendet werden können. Vertrauenswürdiger Anwendungstraffic kann mit direktem Internet-Breakout ohne Umwege über das Internet gesendet werden. Dieser einzigartige Ansatz bietet drei wesentliche Vorteile:

- Identitäts- und anwendungsbasierte Kommunikation statt netzwerkbasierter VPN-Konnektivität für echte Zero-Trust-Sicherheit
- Ersetzt die veraltete Architektur der Abschottung und entsprechende Legacy-Produkte wie Squid-Proxys, NAT-Gateways, IPSs usw., ohne die Sicherheit zu beeinträchtigen
- Für bedarfsgerecht verteilte, skalierbare Verbindungen und eine einheitliche automatische Richtlinienverwaltung zur Vereinfachung der Filial- und RZ-Kommunikation

Anwendungsfälle für Zero Trust SD-WAN

Alternative zu Site-to-Site-VPN

Zweigstellen können ohne WAN oder VPN mit privaten Anwendungen verbunden werden, ohne Ihre Angriffsfläche entsprechend zu vergrößern. Die Anwendungen bleiben hinter den Zweigstellen verborgen und der Zugriff wird mit der Zero Trust Exchange auf bestimmte Entitäten beschränkt. Identität, Kontext und Richtlinieneinhaltung der ausgewählten Teilnehmer werden überprüft, bevor der Zugriff gewährt wird, was die weitere Ausbreitung von Bedrohungen im Netzwerk verhindert.

Fusionen und Übernahmen

Die Zusammenführung von Netzwerken ist kompliziert und zeitaufwendig. Mögliche Komplikationen sind IP-Überschneidungen, Routing-Probleme und ein erhöhtes Sicherheitsrisiko durch die vergrößerte Angriffsfläche. Doch mit Zero Trust SD-WAN können die Netzwerke dauerhaft voneinander getrennt werden. Zweigstellen in der einen Umgebung können aber dennoch schnell und unterbrechungsfrei Verbindungen zu privaten Anwendungen in der anderen Umgebung herstellen.

Direkter Internetzugang für Zweigstellen

Lokale Netzwerk- und Sicherheitsmodelle verlieren an Wirksamkeit, wenn Unternehmen ihre Anwendungen in die Cloud verlagern und cloudnative Anwendungen entwickeln. Zscaler Zero Trust SD-WAN steht dabei für ein neues Modell, bei dem Zweigstellen sicher und unabhängig vom Netzwerk mit jedem beliebigen Ziel kommunizieren können.

Zero Trust für Server und IoT/OT-Geräte

IoT/OT-Ressourcen müssen regelmäßig von Mitarbeitern und Drittanbietern überprüft werden, um ihre Verfügbarkeit zu gewährleisten und Störungen durch Geräte- und Prozessausfälle zu vermeiden. Zero Trust SD-WAN sorgt für einen komplett abgeschotteten, clientlosen Remote-Desktop-Zugriff auf interne RDP- und SSH-Zielsysteme für Vertragspartner und Auftragnehmer. Die Installation eines Clients per Jump-Host oder Legacy-VPN auf dem jeweiligen Gerät ist dabei nicht erforderlich.

Erkennung von Schatten-IoT/OT

IT-Abteilungen übersehen gerne IoT-Geräte, die sich unerlaubt und unerkannt mit dem Niederlassungsnetzwerk verbinden. Doch gerade diese erhöhen die Anfälligkeit der Geräte und vergrößern die Angriffsfläche. Zscaler erkennt und klassifiziert diese Geräte und ermöglicht der IT damit einen umfassenden Überblick in deren Verhalten und bessere Richtlinien für die Zugriffskontrolle.

Z-Connector und Plug-and-Play-Geräte

Funktion	ZT 400	ZT 600	ZT 800	ZT VM
				Z-Connector
Typ	Kleine bis mittelgroße Zweigstellen	Kleine und mittelgroße Niederlassung	Mittelgroße und große Niederlassung	Zweigstelle und Rechenzentrum
Übertragungsrate/ Hypervisor	200 Mbit/s	500 Mbit/s	1 Gbit/s	KVM, ESXi
Physikalische Anschlüsse	4 x GbE	6 x GbE	8 x GbE	N/A
Zero-Touch-Bereitstellung	✓	✓	✓	✓
Detaillierte Weiterleitungsrichtlinien für Internet, private Anwendungen und WAN-Direktverkehr	✓	✓	✓	✓
URL-Filterung, Dateitypkontrolle und Cloud-Firewall-Richtlinien für internetgebundenen Datenverkehr	✓	✓	✓	✓
ZPA-Richtlinien mit Zero Trust für IoT-Geräte und Server	✓	✓	✓	✓
Zentrale Übersicht und Protokollierung	✓	✓	✓	✓

ZSCALER ZERO TRUST SD-WAN: VORTEILE	
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	• Optionale Weiterleitung des Datenverkehrs an ZIA, ZPA oder direkt über das Internet • 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 Datenschutz • Kompletter Security-Stack mit vorkonfigurierter Sicherheit für IoT/OT und Server
Hohe Verfügbarkeit	• Zwei Zero-Trust-SD-WAN-Instanzen im HA-Modus für zusätzliche Unterstützung bei starkem Datenverkehr und Sicherheit bei Hardwareausfällen • Aktiv/Passiv-Fehlertoleranz dank virtueller IP-Adresse (VIP) und Common Address Redundancy Protocol (CARP) • Aktiv-Aktiv-Schaltungen (Einzelgerät) • Aktiv-Aktiv-Schaltungen (Dual-Appliance bei FHRP-Lastausgleich)
Zentrale Übersicht und genaue 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 • Lückenlose Einbindung in den Nanolog Streaming Service mit optionalem Protokollstreaming an das kundenseitige SIEM
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

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.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.de