DATENBLATT

Zscaler Private Access™

Bieten Sie Ihrer Belegschaft schnellen, sicheren und zuverlässigen Zugriff auf private Unternehmensanwendungen mit der branchenweit ersten KI-gestützten ZTNA-Lösung.

Zscaler Private Access (ZPA) ist eine Cloud-native Lösung, die allen Usern Zero-Trust-Zugriff mit direkter Konnektivität zu privaten Unternehmensanwendungen bereitstellt und gleichzeitig die Angriffsfläche minimiert, laterale Bewegungen eliminiert und vor komplexen Angriffen schützt.

Herkömmliche Netzwerksicherheitsansätze erfüllen die Anforderungen Ihrer hybriden Belegschaft und Ihres Unternehmens nicht. Herkömmliche Firewalls und VPNs bieten Angreifern eine riesige Angriffsfläche, die sie finden und ausnutzen können. Außerdem lassen sie User direkt auf Ihr Netzwerk zugreifen, was eine laterale Ausbreitung von Bedrohungen ermöglicht. Wenn die Anmeldeinformationen Ihres Users kompromittiert werden, haben Angreifer einfachen Zugriff auf Ihre vertraulichen Daten. Die Verwendung eines VPN, um Ihrer hybriden Belegschaft und Drittanbietern Zugriff zu ermöglichen, erhöht das Cyberrisiko, führt zu schlechten Usererfahrungen und erhöht den Verwaltungsaufwand. Um Usern von jedem Gerät und Standort aus sicheren Zugriff zu ermöglichen, benötigen Sie einen effektiveren Ansatz.

Bis 2025 werden laut Gartner mindestens 70 % der neuen Bereitstellungen von Remotezugriff nicht mehr über VPN-Services, sondern überwiegend über Zero Trust Network Access (ZTNA) abgewickelt werden. Ende 2021 waren es noch weniger als 10 %.

Vorteile:

- **Ersetzen Sie anfällige VPN-Lösungen.**Reduzieren Sie die Angriffsfläche und verhindern Sie seitliche Bewegungen, indem Sie User direkt mit Anwendungen verbinden — nicht mit dem Netzwerk. Verbessern Sie so Ihre Sicherheitslage.
- **Verhindern Sie Cyberangriffe.**Minimieren Sie das Risiko eines Verstoßes mit privatem App-Schutz vor Web- und Identitätsbedrohungen, erweitertem Bedrohungsschutz mit vollständiger Inline-Prüfung und Verhinderung von Datenverlust.
- **Unterstützung für hybride Belegschaften.**Erweitern Sie nahtlos und blitzschnell den Zugriff auf private Unternehmensanwendungen für alle User, die Zentrale, Zweigstellen und Drittanbieter.
- **Weniger betriebliche Komplexität**Bieten Sie sicheren, optimierten Zugriff ohne kostspielige und komplexe Einzelprodukte über eine einheitliche, Cloud-native ZTNA-Plattform für User, Workloads und OT/IT

Legacy-Ansätze zur Netzwerksicherheit können leicht umgangen werden, indem Angreifer das inhärente Vertrauen und unnötige Zugriffsberechtigungen herkömmlicher Architekturen nach dem Festung-mit-Burggraben-Prinzip ausnutzen:

- **Legacy-Architekturen sind nicht skalierbar und bieten keine schnelle, nahtlose User Experience:** VPNs erfordern Backhauling, was Kosten, Komplexität und zu hohe Latenzen für Remote-Mitarbeiter mit sich bringt.
- **Herkömmliche Firewalls, VPNs, VDI und private Anwendungen schaffen eine große Angriffsfläche:** Angreifer können anfällige, von außen zugängliche Ressourcen entdecken und ausnutzen.
- **Durch den Zugriff auf das gesamte Netzwerk können sich Angreifer ungehindert lateral bewegen:** VPNs lassen User in Ihr Netzwerk gelangen, wodurch Angreifer leichten Zugang zu sensiblen Daten erhalten.
- **Kompromittierte User und Insider-Bedrohungen können herkömmliche Kontrollen umgehen:** Versierte Angreifer können Anmeldeinformationen stehlen und Identitäten missbrauchen, um mit herkömmlichen Tools für den Remote-Zugriff auf private Unternehmensanwendungen zuzugreifen.

Es ist an der Zeit zu hinterfragen, wie man User sicher und reibungslos mit den Anwendungen verbinden kann, die sie benötigen. Außerdem muss die Sicherheit privater Anwendungen mit ZTNA neu definiert werden.

Zscaler Private Access™ (ZPA)

Zscaler Private Access (ZPA), der erste KI-gestützte ZTNA der Branche, ist eine Cloud-native Lösung, die allen Usern Zero-Trust-Zugriff mit direkter Konnektivität zu privaten Unternehmensanwendungen bietet und gleichzeitig die Angriffsfläche minimiert, indem Apps hinter der Zero Trust Exchange verborgen werden. Laterale Bewegungen werden durch KI-gestützte User-zu-App-Segmentierung eliminiert und durch integrierte Traffic-Überprüfung sowie Anwendungsschutz und Data Protection vor komplexen Angriffen geschützt. Als resilienter Cloud-nativer Service, der auf einem ganzheitlichen SSE-Framework (Security Service Edge) basiert, kann ZPA in wenigen Stunden bereitgestellt werden, um Legacy-VPNs und -Tools für den Remotezugriff zu ersetzen. Dadurch können folgende Vorteile erzielt werden:

- **Minimierte Angriffsfläche:** Die Anwendungen sind für das Internet unsichtbar, sodass nicht autorisierte User und Geräte sie nicht entdecken können. Die Inside-Out-Verbindungen zwischen User und Anwendung stellen sicher, dass Anwendungen und IPs niemals offengelegt werden.
- **Durchsetzung minimaler Zugriffsrechte:** Der Anwendungszugriff wird durch Identität und Kontext bestimmt — nicht durch eine IP-Adresse — und User erhalten niemals Zugriff auf das Netzwerk.
- **Unterbindung von lateralen Bewegungen:** Anwendungen werden so segmentiert, dass User nur auf eine bestimmte Anwendung zugreifen können, was die lateralen Bewegungsmöglichkeiten einschränkt.
- **Schutz vor Cyberangriffen durch vollständige Überprüfung:** Der Traffic privater Anwendungen wird inline überprüft, um die gängigsten Angriffsmethoden zu verhindern.
- **Vermeidung von Datenverlusten:** Integrierte DLP für private Anwendungen, fortschrittliche Reaktion auf Vorfälle und Datenklassifizierung zum Schutz der wichtigsten Anwendungen
- **Hervorragende User Experience:** Durch die direkte Verbindung von Usern mit privaten Anwendungen entfällt das langsame, kostspielige Backhauling über herkömmliche VPNs, während Probleme mit der User Experience kontinuierlich überwacht und proaktiv gelöst werden.

Schätzungen zufolge werden bereits 2025 mindestens 70 % aller neuen Remotezugriff-Bereitstellungen überwiegend über ZTNA (statt über VPN-Services) abgewickelt. Ende 2021 waren es noch weniger als 10 %.*

— Gartner

*Gartner, Emerging Technologies: Adoption Growth Insights for Zero Trust Network Access, Nat Smith, Mark Wah, Christian Canales. 8. April 2022

Die wichtigsten Anwendungsfälle

Sicherer Fernzugriff (VPN-Ersatz)
Über die Cloud oder Appliances bereitgestellte VPNs setzen Sie Cyberangriffen aus. Sie sind voller Schwachstellen und werden regelmäßig von Angreifern ausgenutzt. Ihr netzwerkzentriertes Design leitet den Datenverkehr zurück, erweitert die Angriffsfläche und ermöglicht laterale Bewegungen, indem User direkt in das Netzwerk gesteckt werden, was zu Ransomware-Angriffen führt. VPNs sind unsicher, langsam und komplex zu verwalten.

ZPA löst diese Herausforderungen, indem es allen Usern Zero-Trust-Zugriff mit direkter Konnektivität zu privaten Unternehmensanwendungen bietet und gleichzeitig die Angriffsfläche minimiert, indem Apps hinter der Zero Trust Exchange verborgen werden. Laterale Bewegungen werden durch KI-gestützte User-zu-App-Segmentierung eliminiert und durch integrierte Traffic-Überprüfung sowie Anwendungsschutz und Data Protection vor komplexen Angriffen geschützt. ZPA bewältigt diese Herausforderungen, indem die Lösung schnellen, direkten Zugriff auf Anwendungen über mehr als 160 weltweit verteilte Points of Presence (PoPs) ohne die mit VPN verbundenen Sicherheitsrisiken bietet. Das Cloud-native Design von ZPA hat den Vorteil, dass IT-Teams auf Inbound-Gateway-Appliances wie Load Balancer, VPN-Konzentratoren und andere Sicherheitsgeräte verzichten können, was Kosten, Komplexität und Verwaltungsaufwand reduziert. ZPA bietet Zero-Trust-Zugriff auf alle Anwendungen, einschließlich netzwerkverbundener Anwendungen wie Voice over IP (VoIP) und Server-zu-Client-Anwendungen und sogar von Geschäftspartnern gehosteter (Extranet-)Anwendungen, bei denen Kunden die Anwendungskonnektoren der Lösung nicht bereitstellen können.

Sicherer App-Zugriff für User im Büro und Hybrid-User
In der modernen Arbeitswelt arbeiten User von zu Hause und anderen entfernten Standorten, Zweigstellen und der Zentrale aus, was veraltete Sicherheitsparadigmen in Frage stellt. Unternehmen benötigen unterbrechungsfreien Zugriff auf Anwendungen, ohne die Zero-Trust-Sicherheit bei Katastrophen oder Zeiten eingeschränkten Infrastrukturzugriffs zu gefährden. Compliance- und regulatorische Standards müssen zur Gewährleistung der Geschäftskontinuität eingehalten werden.

Mit ZPA Private Service Edge können Sie die Leistung der Cloud auch On-Premise nutzen und dieselben Sicherheitskontrollen wie für Ihre Remote-User mit derselben hohen Performance durchsetzen. Durch die Bereitstellung von Zscaler Private Service Edges mit privaten Cloud-Controllern unterstützt ZPA bei Erkennung eines Ausfalls die vollständig automatisierte Umstellung in den Business Continuity-Modus. Richtlinien und Authentifizierung werden durchgesetzt, auch wenn die ZPA-Cloud nicht erreichbar ist.

BYOD und Userzugriff durch Drittanbieter:
Der herkömmliche Zugriff durch Drittanbieter basierte auf kostspieligen, komplexen und riskanten Lösungen wie VDI, RDP, SSH oder VNC, die den Usern direkten Zugriff auf das Netzwerk gewährten und interne Systeme nicht vertrauenswürdigen Geräten aussetzten.

Die Clientless-Access-Funktionen von ZPA ermöglichen mühelosen Drittanbieterzugriff, senken Kosten und minimieren Risiken. Dritte wie Auftragnehmer, Lieferanten und Partner können mit jedem beliebigen Webbrowser auf ihren eigenen Geräten eine Verbindung zu Intranet-Websites, internen Systemen und Geräten herstellen — kein Client erforderlich. Dritt-User und nicht verwaltete Geräte werden von Ihrem Netzwerk und Ihren Anwendungen isoliert, sodass vertrauliche Daten vor unbefugtem Kopieren/Einfügen, Drucken und Hoch- bzw. Herunterladen geschützt sind. Die Integration von ZPA und Google Chrome Enterprise Browser erhöht die Sicherheit für nicht verwaltete bzw. BYOD-Geräte durch Überprüfung des Chrome-Enterprise-Browsers und Einbeziehung zusätzlicher Posture-Informationen in ZPA-Richtlinienprüfungen. Mit Clientless Access kann die IT den Usern ein besseres und sichereres Erlebnis bieten, ohne die Kosten für die Verwaltung herkömmlicher VDI tragen zu müssen. Fusionen, Übernahmen und Veräußerungen stellen eine Herausforderung für die Netzwerkintegration dar, aber ZPA beschleunigt diesen Prozess von Monaten auf Wochen. ZPA bietet nahtlosen Zugriff auf private Unternehmensanwendungen sodass keine Netzwerkkonvergenz oder zusätzliche Geräte erforderlich sind.

Sicherer berechtigungsbasierter Zugriff auf OT und IIoT
Mitarbeiter und Drittanbieter müssen regelmäßig auf OT- und IIoT-Ressourcen zugreifen, um Produktionszeiten zu maximieren und Unterbrechungen durch Geräte- und Prozessausfälle zu vermeiden. ZPA ermöglicht einen schnellen, sicheren und zuverlässigen Zugriff auf OT- und IIoT-Umgebungen an Außenstandorten, in der Fabrikhalle und an jedem anderen Ort. ZPA für IoT & OT bietet vollständig isolierten, clientlosen Remote-Desktop-Zugriff auf interne RDP-, SSH- und VNC-Zielsysteme — ohne dass User einen Client mit Jump-Hosts und Legacy-VPNs auf ihrem Gerät installieren müssen.

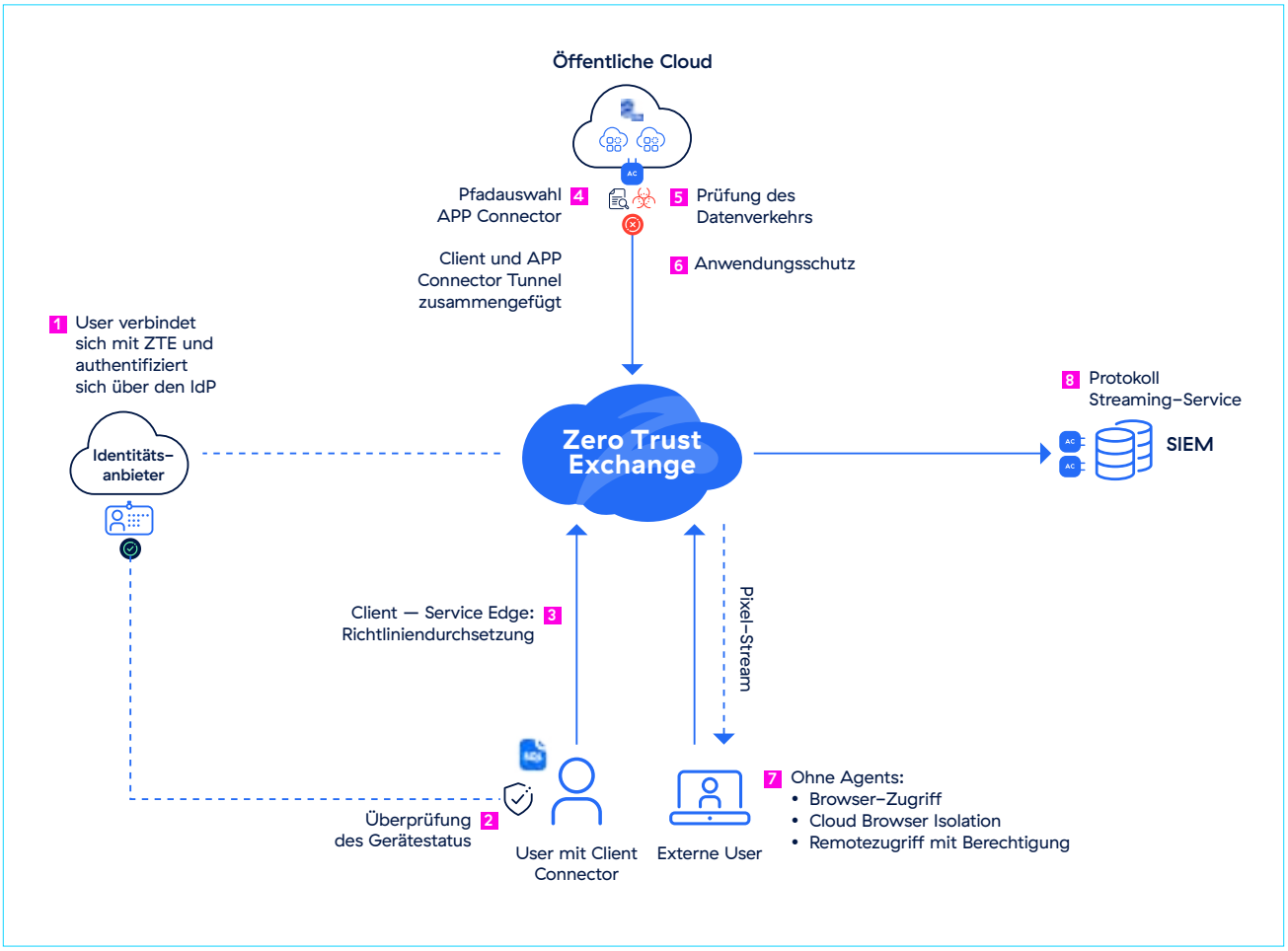
VDI-Alternative:
IT- und Sicherheitsteams haben keine Kontrolle über nicht verwaltete Geräte, was Geschäftsrisiken birgt. Um den Anwendungszugriff auf nicht verwalteten Geräten zu unterstützen, haben Unternehmen traditionell VDI verwendet. VDIs stellen User direkt auf das Netzwerk und setzen interne Anwendungen nicht verwalteten Endpunkten aus. Darüber hinaus sind VDIs teuer, umständlich zu verwalten und nicht skalierbar. Im Zuge der digitalen Transformation sind modernisierte Anwendungen in der Regel web- oder browserbasiert, und das Streamen eines gesamten Desktops über VDI bietet kein besonders gutes EndUsererlebnis.

ZPA ist eine effektive VDI-Alternative, die sicheren, agentenlosen, browserbasierten Zugriff auf nicht verwaltete Geräte bietet. User erhalten schnellen und nahtlosen Zugriff auf private Unternehmensanwendungen über den nächstgelegenen Service-Edge. Die ZPA-Architektur bietet Direktzugriff auf Anwendungen, ohne dass der User in das Netzwerk eingebunden werden muss, und gewährleistet dadurch sicheren Zugriff auf private Unternehmensanwendungen. Mit ZPA Browser Access können User einen Webbrowser zur Userauthentifizierung und zum Anwendungszugriff nutzen, ohne dass der Zscaler Client Connector auf ihren Geräten installiert sein muss. ZPA verfügt über eine integrierte Browser-Isolierung, wodurch nicht der eigentliche Inhalt, sondern nur Pixel auf das Endgerät des Nutzers gestreamt werden; die Daten innerhalb der Apps bleiben somit geschützt. Mit ZPA können Administratoren Isolationsrichtlinien erstellen, um zu definieren, wie ein User innerhalb der isolierten Umgebung interagieren kann.

Mikrosegmentierung
Remote-Access-Lösungen wie VPNs gewähren vollständigen Netzwerkzugriff und stellen IPs und Anwendungen dem Internet zur Verfügung. VPNs erweitern das interne Netzwerk auf Remote-Geräte und erfordern von Natur aus eingehenden Traffic, wodurch eine öffentliche Angriffsfläche entsteht. Ohne ordnungsgemäße Netzwerksegmentierung könnte ein Verstoß in einem Segment das gesamte Netzwerk des Unternehmens gefährden. Allerdings erfordert die Implementierung der Segmentierung komplexe Firewall-Regeln, die schwer zu verwalten sind, häufig Anwendungen stören und den Zugriff für VPN-User erschweren können. In großen Organisationen erfordert dies häufig hohe Verfügbarkeit, komplexes Routing und kostspielige private Verbindungen.

Die KI-gestützte App-Segmentierung von Zscaler bietet eine präzise User-zu-App-Segmentierung und eine robuste Lösung für die einfache Bereitstellung konsistenter Richtlinien im großen Maßstab und die Verhinderung lateraler Bedrohungsausbreitungen. Sie unterstützt Sie dabei, den Überblick alle Anwendungen in Ihrem Unternehmen zu erhalten, und bietet visuelle Einblicke, welche User Zugriff auf welche Anwendungen haben. Sie generiert automatisch Empfehlungen für App-Segmente und Richtlinien auf Grundlage von Modellen des maschinellen Lernens und vereinfacht so die Implementierung.

Wie ZPA funktioniert



Funktionsweise

Wenn ein User (Mitarbeiter, Anbieter, Partner oder Auftragnehmer) versucht, auf eine interne Anwendung zuzugreifen, bietet ZPA eine sichere, direkte Verbindung durch folgende Schritte:

1 Der User stellt über den Client Connector eine Verbindung zur Zero Trust Exchange her und authentifiziert sich beim Identitätsanbieter (IdP). Nach erfolgreicher Authentifizierung wird die Verbindung zum Public Service Edge wieder hergestellt und eine einzelne, permanente TLS-Verbindung zum Service Edge eingerichtet.

2 Nach der Userauthentifizierung und dem Tunnelaufbau zum Service Edge lädt der Client-Connector seine Konfiguration herunter, einschließlich der Gerätestatusprüfung.

3 Die Zscaler App leitet den User-Traffic an die nächstgelegene ZPA Service Edge weiter, die als Broker fungiert. Dort werden die Sicherheits- und Zugriffsrichtlinien des Users überprüft.

4 Zwei ausgehende Tunnel, einer vom Client Connector auf dem Gerät, der andere vom App Connector, werden von der ZPA Service Edge zusammengeführt.

5 Sobald eine Verbindung zwischen dem Gerät des Users und der Anwendung hergestellt wurde, prüft App Connector automatisch den Traffic inline, um potenzielle Bedrohungen durch User oder Geräte zu erkennen und abzuwehren.

6 Zscaler AppProtection schützt private Unternehmensanwendungen vor dem Web und auf Identitätsbasis durch eine umfassende Layer-7-Prüfung und verbessert so den allgemeinen Sicherheitsstatus.

7 Darüber hinaus können externe User mithilfe von integriertem browserbasiertem Zugriff oder Zscaler Browser Isolation agentenlos über nicht verwaltete Geräte auf private Unternehmensanwendungen zugreifen.

8 Log Streaming Service (LSS) überträgt verschiedene Protokolle, einschließlich der Useraktivität, an SIEM.

Ein ZPA Service Edge kann entweder von Zscaler in der Cloud gehostet (ZPA Public Service Edge) oder vor Ort in Ihrer Infrastruktur ausgeführt werden (ZPA Private Service Edge). Dies bietet einen kürzeren Pfad zu lokalen Apps und unterstützt die Geschäftskontinuitätsplanung.

Die wichtigsten Funktionen

Risikobasierte Richtlinien-Engine	Überprüfung von Zugriffsrichtlinien auf Grundlage von User-, Geräte-, Inhalts- und Anwendungsrisiken mit einer leistungsstarken nativen Policy-Engine, damit nur authentifizierte User auf private Anwendungen zugreifen können.
Einheitlicher Zugriff mit und ohne Client	Um optimalen Schutz für hybride IT-Umgebungen zu gewährleisten, stehen mehrere Schutzmethoden zur Auswahl. Die clientbasierte Option schützt User mit verwalteten Geräten auch außerhalb des Unternehmensnetzwerks mit einem ressourcenschonenden Agent, dem Zscaler Client Connector. Die clientlose Option gewährleistet reibungslosen Zugriff für User mit nicht verwalteten Geräten unabhängig vom verwendeten Gerät und Webbrowser.
Browser Access	BYOD- und externe User können ihre privaten Geräte nutzen, um über einen beliebigen Webbrowser nahtlos und sicher auf interne Anwendungen zuzugreifen, ohne dass ein Client erforderlich ist.
Lokaler ZTNA	Mithilfe von lokalem ZTNA können Sie User sicher mit Anwendungen in Ihren Büros verbinden. Zugriff und Richtliniendurchsetzung erfolgen konsistent und unabhängig vom Standort der User oder der Anwendungen.
Business Continuity und Notfallwiederherstellung	Profitieren Sie von ununterbrochenem Zugriff auf geschäftskritische Anwendungen, selbst im Fall von unvorhergesehenen Katastrophen, mit einer kundenseitig gesteuerten Business-Continuity-Lösung, die den Zugriffspfad zu kritischen privaten Unternehmensanwendungen über ZPA Private Service Edge bereitstellt.
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 Anwendungssegmentierung	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.
User-zu-App-Segmentierung	Stellen Sie sicher, dass der gesamte Anwendungszugriff nach Erforderlichkeitsprinzip mit minimaler Rechtevergabe und User-to-App-Segmentierung gewährt wird. Stellen Sie autorisierten Usern sicheren Zugriff auf bestimmte festgelegte Anwendungen bereit, ohne dass User ins Netzwerk gelangen. Verzichten Sie auf eine komplizierte Netzwerksegmentierung mit internen Firewalls.
Anwendungsschutz	Schützen Sie private Anwendungen und Infrastruktur mit einer leistungsstarken Inline-Sicherheitsüberprüfung der gesamten Anwendungsnutzungsdaten vor den gängigsten Angriffsmethoden. Erkennen und blockieren Sie bekannte Websicherheitsrisiken, wie z. B. die OWASP Top 10, sowie neuartige Zero-Day-Bedrohungen, die herkömmliche Netzwerksicherheitskontrollen umgehen können.

Remotezugriff mit minimaler Rechtevergabe	Stellen Sie autorisierten Administratoren und Mitarbeitern eine sichere Verbindung zu Intranet-Websites, internen Systemen und Geräten ohne die Notwendigkeit von VPNs, VDIs oder Remote-Desktop-Clients wie RDP, SSH und VNC bereit.
Bedrohungsabwehr und Data Protection	Weniger Bedrohungsrisiken dank vollständiger Inhaltsüberprüfung. Identifizieren und Kontrollieren sensibler Daten in Verbindungen zwischen Usern und Anwendungen.
Identität und Single Sign-On (SSO)	Einfache Integration in Ihre vorhandene Identitäts- und Authentifizierungsinfrastruktur und Nutzung von SSO zur weiteren Reduzierung der Komplexität.
Sicherer Zugriff auf Netzwerk-Apps	Aktivieren Sie diese Option, um den Zugriff auf ältere, mit dem Netzwerk verbundene Anwendungen wie VoIP und Server-zu-Client-Anwendungen zu sichern.
IPsec-Konnektivität	Ermöglichen Sie Zero-Trust-basierten Zugriff auf Anwendungen von Geschäftspartnern und Anbietern (Extranet-Anwendung), die in ihren Netzwerken gehostet werden

Geschäftsnutzen

Minimierung der Angriffsfläche Indem anfällige VPNs abgeschafft und Anwendungen für das Internet unsichtbar gemacht werden, wird es für unbefugte User unmöglich, sie zu finden und anzugreifen. ZPA erstellt ein Segment zwischen einem autorisierten User und einer bestimmten privaten Anwendung, wobei alle eingehenden Verbindungen unterbunden und nur Inside-Out-Verbindungen über verschlüsselte Mikrotunnel zu den Geräten der User zugelassen werden. Administratoren können mithilfe der Anwendungserkennung automatisch gefährliche Anwendungen, Services sowie Workloads erkennen und segmentieren und so die Angriffsfläche weiter verringern.

Vermeiden Sie laterale Bewegungen. Konnektivität basierend auf dem Zugriff mit den geringsten Berechtigungen stellt sicher, dass der Anwendungszugriff von einem autorisierten User auf benannte Anwendungen eins zu eins gewährt wird, anstatt Vollzugriff auf das Netzwerk zu gewähren. Daher ist laterale Bewegung zwischen Apps oder über das Netzwerk unmöglich. Da ZPA nicht auf IP-Adressen basiert, entfällt die Notwendigkeit, komplexe Netzwerksegmentierung, Zugriffskontrolllisten (ACLs), Firewall-Richtlinien oder Netzwerkadressübersetzungen einzurichten und zu verwalten.

Verhindern Sie kompromittierte User, Insider-Bedrohungen und fortgeschrittene Angreifer. Integrierte Inline-Inspektion und DLP-Funktionen minimieren das Risiko kompromittierter User und aktiver Angreifer. ZPA stoppt automatisch Webangriffe mit vollständiger Abdeckung der gängigsten Techniken, einschließlich der OWASP Top 10, und vollständiger Unterstützung Userdefinierter Signaturen für sofortiges virtuelles Patchen gegen Zero-Day-Schwachstellen. ZPA minimiert Risiken durch Drittanbieter und BYOD durch vollständig isolierten Zugriff auf Anwendungen, der vertrauliche Daten mithilfe der integrierten Cloud-Browser-Isolierung von nicht verwalteten Geräten fernhält.

Bereitstellung einer hervorragenden User Experience Dank der durchgängig schnellen Konnektivität, die keine An- und Abmeldung bei VPN-Clients erfordert, können Remote-User sicherer und effizienter auf Ressourcen zugreifen. Auftragnehmer, Lieferanten und Partner profitieren von reibungslosem Zugriff über jedes Gerät und jeden Webbrowser, ohne einen Client installieren zu müssen. User melden sich einfach mit ihren bestehenden SSO-Anmeldedaten an (Azure AD, Okta, Ping usw.). Darüber hinaus können Administratoren die Produktivität der User fördern, indem sie Performanceprobleme bei Endusern, die durch Schwierigkeiten beim Zugriff auf private Unternehmensanwendungen, Ausfälle von Netzwerkpfaden oder Netzwerküberlastungen verursacht werden, proaktiv erkennen und beheben.

Eine einheitliche Plattform für sicheren Zugriff für alle Anwendungen, Workloads und Geräte Erweitern Sie Zero Trust auf private Unternehmensanwendungen, Workloads und OT-/IoT-Geräte, um verschiedene unzusammenhängende Tools für den Remote-Zugriff zu integrieren sowie Sicherheits- und Zugriffsrichtlinien zu standardisieren, um Verstöße zu verhindern und die betriebliche Komplexität zu reduzieren.

Bundle-Optionen für Zscaler Private Access

	Zscaler Essentials Platform (ZS-ESS-PLATTFORM)	Zscaler Private Access Platform (ZS-ZPA-PLATFORM)	Zscaler Plattform (ZS-PLATFORM)
Private Access Platform Services			
Granulare Zugriffskontrolle nach User, Gruppe und Ports	ja 1 User pro 20 angemeldete User (Mindestens 500 angemeldete User)	ja	ja
Protokoll Streaming-Service			
Permanente Zustandsüberwachung für alle Applikationen			
Source IP Anchoring			
App Connector	$	So viele wie nötig, bis zum Systemmaximum	So viele wie nötig, bis zum Systemmaximum
ZPA Private Service Edge			
Zugang von Drittparteien			
Browserbasierter Zugriff	$	ja PRA für mehr als 500 User	ja PRA für mehr als 500 User
User-Portal			
Privileged Remote Access (PRA) Standard			
Digital Experience Monitoring			
ZDX Standard	$	ja	ja
Sicherheit für private Unternehmensanwendungen			
Data Protection für private Unternehmensanwendungen	$	$	ja Deception für mehr als 500 User
Risikomanagement: Deception			
Segmentierung			
Vorschau für App-Segmente und Segmentierung	20 Anwendungssegmente (10 Empfehlungen/90 Tage, eingeschränkte Rückschau)	20 Anwendungssegmente (10 Empfehlungen/90 Tage, eingeschränkte Rückschau)	20 Anwendungssegmente (10 Empfehlungen/90 Tage, eingeschränkte Rückschau)
Segmentierungs-Add-On			
Unbegrenzte Anzahl von Anwendungssegmenten	ja 100 Empfehlungen/14 Tage Wöchentliche Berichte auf Abruf, Herunterladen und Analysieren von Daten von bis zu 30 Tagen Importieren von Apps aus internen Systemen oder Quellen von Drittanbietern (Qualys, Tenable, ServiceNow).	ja 100 Empfehlungen/14 Tage Wöchentliche Berichte auf Abruf, Herunterladen und Analysieren von Daten von bis zu 30 Tagen Importieren von Apps aus internen Systemen oder Quellen von Drittanbietern (Qualys, Tenable, ServiceNow).	ja 100 Empfehlungen/14 Tage Wöchentliche Berichte auf Abruf, Herunterladen und Analysieren von Daten von bis zu 30 Tagen Importieren von Apps aus internen Systemen oder Quellen von Drittanbietern (Qualys, Tenable, ServiceNow).
KI-gestützte Segmentierung			
Analyse-basierte Segmentierung			
App-Segmente importieren (aus strukturierten Datendateien)			
Add-on: AppProtection			
Sichtbarkeit von Angriffen auf Anwendungen	Add-on	Add-on	Add-on
OWASP Top 10 Abwehrmaßnahmen: SQL-Injection, Cross-Site-Scripting, Umgebungs- und Port-Scanner			
Schutz vor Zero-Day-Bedrohungen			
Überwachung hochriskanter User			

Wichtige Unterscheidungsmerkmale

Als branchenweit erste KI-gestützte ZTNA-Lösung bietet ZPA höchste Sicherheit mit einer erstklassigen User Experience:

- **Von Grund auf für den Zugriff mit minimaler Rechtevergabe entwickelt:** Autorisierte User können nur auf genehmigte Ressourcen zugreifen, nicht auf Ihr Netzwerk — was mit herkömmlichen VPNs unmöglich wäre.
- **Anwendungen werden für Angreifer unsichtbar und unzugänglich:** Wenn private Unternehmensanwendungen für das öffentliche Internet unsichtbar sind, können kompromittierte Anwendungen, Datendiebstahl und laterale Bewegungen verhindert werden.
- **Vollständige Inline-Überprüfung:** Schützen Sie Ihre Anwendungen, indem Sie den Missbrauch privater Anwendungen erkennen und unterbinden. So verhindern Sie automatisch die gängigsten Webangriffe und schützen Ihre Daten mit branchenführender DLP.
- **Globale Geschäftskontinuität ohne Kompromisse bei der Sicherheit:** Minimieren Sie die Auswirkungen von Störungen und erzwingen Sie Zero-Trust-Zugriff, um strenge Compliance-Anforderungen zu erfüllen, selbst wenn die Zscaler-Cloud nicht erreichbar ist.
- **Clientloser Zugriff:** Nutzen Sie den browserbasierten Zugriff für externe User mit integrierten DLP-Funktionen.
- **Eliminieren Sie laterale Bewegungen mit KI-gestützter Segmentierung:** Bietet präzise User-zu-App-Segmentierung, visualisiert den Zugriff und optimiert Richtlinien mithilfe von maschinellem Lernen, um Angriffsflächen zu minimieren und laterale Bedrohungen zu verhindern.
- **Globale Edge-Präsenz:** Profitieren Sie von unübertroffener Sicherheit und User Experience mit mehr als 160 Cloud-Edge-Standorten weltweit sowie einem optionalen lokalen Service Edge, um Zero Trust auf Ihre Zentrale auszuweiten.
- **Cloud-native Grundlage:** Die in der Cloud bereitgestellte Plattform wächst skalierbar mit dem Unternehmen mit, das so auf kostspielige On-Premise-Hardware oder komplexe Infrastruktur verzichten kann.
- **Einheitliche ZTNA-Plattform für User, Workloads und Geräte:** Mit der umfassendsten ZTNA-Plattform der Branche können Sie sicher auf private Anwendungen, Services und OT-Geräte zugreifen.
- **Teil einer erweiterbaren Zero-Trust-Plattform:** Die Zero Trust Exchange basiert auf einem vollständigen SSE-Framework und bietet Schutz und Unterstützung für Unternehmen.

**Gartner, Magic Quadrant for Security Service Edge, Charlie Winckless, Thomas Lintemuth, Dale Koeppen, 15. April 2024

Gartner unterstützt keine Anbieter, Produkte oder Dienstleistungen, die in seinen Forschungspublikationen aufgeführt sind, und empfiehlt Technologieanwendern nicht, nur Anbieter mit den höchsten Bewertungen auszuwählen. Publikationen von Gartner spiegeln die Ansichten von Gartners Forschungsunternehmen wider und sollten nicht als Tatsachenfeststellungen interpretiert werden. Gartner übernimmt keinerlei ausdrückliche oder stillschweigende Gewähr in Bezug auf diese Studie, insbesondere in Bezug auf Angaben zur Marktgängigkeit oder Eignung für einen bestimmten Zweck.

GARTNER ist eine eingetragene Marke und Dienstleistungsmarke von Gartner, Inc. und/oder den mit ihm verbundenen Unternehmen innerhalb und außerhalb der USA; MAGIC QUADRANT ist eine eingetragene Marke von Gartner, Inc. und/oder seinen Tochtergesellschaften. Sie werden hierin mit Genehmigung verwendet. Alle Rechte vorbehalten.

Grundlegende Komponenten

Zscaler Client Connector
Client Connector ist eine schlanke Anwendung, die auf den Laptops und Mobilgeräten der User ausgeführt wird. Durch die automatische Weiterleitung des User-Traffics an die nächstgelegene Zscaler Service Edge wird sichergestellt, dass Sicherheits- und Zugriffsrichtlinien über alle Geräte, Standorte und Anwendungen hinweg durchgesetzt werden.

Zscaler Clientless Access
User können über den integrierten browserbasierten Zugriff (Web, RDP, SSH, VNC) oder Zscaler Browser Isolation für den clientlosen Zugriff auf nicht verwalteten Geräten eine sichere Verbindung zu Anwendungen, Workloads und OT-Geräten herstellen.

ZPA App Connector
App Connectors sind ressourcenschonende virtuelle Maschinen, die privaten Anwendungen im Rechenzentrum oder in öffentlichen Cloud-Umgebungen vorgeschaltet werden. Sie ermöglichen befugten Usern den Zugriff auf spezifische Anwendungen über ausgehende Verbindungen, sodass die Anwendung nicht im Internet exponiert wird.

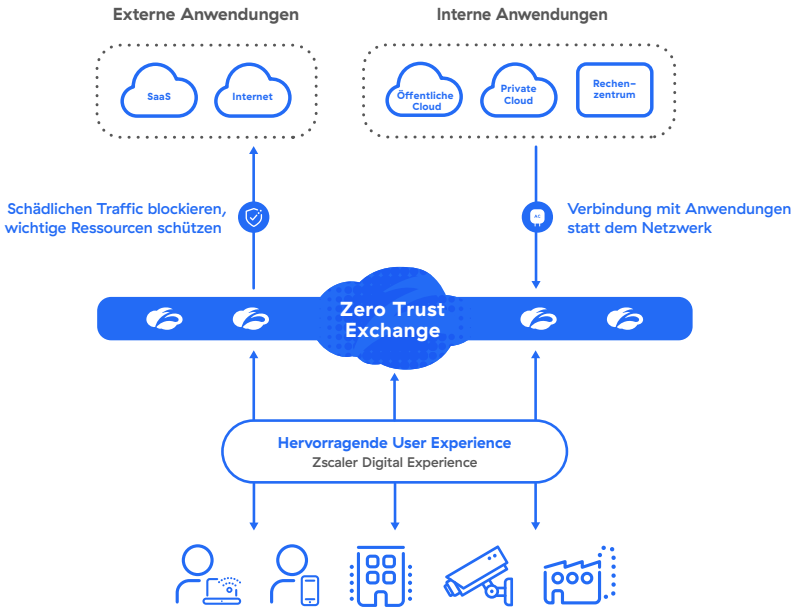
ZPA Service Edges
Service Edges setzen Sicherheits- und Zugriffsrichtlinien durch und stellen die Inside-Out-Verbindung zwischen einem autorisierten User (über Client Connector und Browser Access) und einer bestimmten privaten Anwendung (über App Connector) her. Die meisten Kunden nutzen unsere Public Service Edges, die in mehr als 160 Knotenpunkten auf der ganzen Welt gehostet werden und Millionen von Usern für die größten Unternehmen der Welt bedienen. Private Service Edges, die von Zscaler verwaltet werden, können auch vor Ort gehostet werden, um On-Premise-Usern den kürzesten Weg zu On-Premise-Anwendungen bereitzustellen, ohne das lokale Netzwerk zu verlassen.

ZPA ist Teil der ganzheitlichen Zero Trust Exchange

Die Zscaler Zero Trust Exchange ist eine Cloud-native Plattform, die eine vollständige Security Service Edge (SSE) bereitstellt, um User, Workloads und Geräte miteinander zu verbinden, ohne ihnen Zugang zum Unternehmensnetzwerk zu gewähren. Perimeterbasierte Sicherheitslösungen vergrößern Netzwerk und Angriffsfläche, erhöhen das Risiko der lateralen Ausbreitung von Bedrohungen und können Datenverluste nicht verhindern. Die Zero Trust Exchange hingegen minimiert all diese Sicherheitsrisiken und die damit einhergehende Komplexität.

Zero Trust für User, Workloads und IIoT/Betriebstechnologie (OT) — mit Zscaler

Bereitstellung innerhalb weniger Wochen zur Verbesserung der Cybersicherheit und Anwendererfahrung



Technische Spezifikationen

Zscaler-Komponente	Unterstützte Plattformen und Systeme	
Client Connector	iOS 9 oder höher Android 5 oder höher Windows 7 oder höher	macOSX 10.10 oder höher CentOS 8 Ubuntu 20.04
Clientloser Zugriff	Moderne Webbrowser: (HTML-5-fähig)	Chrome Edge Firefox
App Connector	AWS Centos, Oracle und Red Hat Microsoft Azure	Microsoft Hyper-V VMware vCenter oder vSphere Hypervisor Docker-Host

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