Datenblatt

Zscaler Private Access™

Bieten Sie Ihrer Belegschaft schnellen, sicheren und zuverlässigen Zugriff auf private Anwendungen mit der branchenweit ersten und einzigen ZTNA-Lösung der nächsten Generation.

Zscaler revolutioniert den Zugriff auf private Anwendungen mit fortschrittlichen Funktionen für Konnektivität, Segmentierung und Sicherheit. So können Sie Ihr Unternehmen vor Bedrohungen schützen und Ihren Usern gleichzeitig eine optimale User Experience bereitstellen.

Veraltete Netzwerk- und Sicherheitsansätze werden den Anforderungen der modernen hybriden Belegschaften nicht gerecht

Die Verbindung von Usern mit privaten Anwendungen sollte nicht langsam, kompliziert oder riskant sein. Hybrides Arbeiten und die Cloud-Transformation haben perimeterbasierte Netzwerksicherheitsmodelle auf den Kopf gestellt. Private Anwendungen werden in die Cloud verlagert und User greifen über das öffentliche Internet auf Anwendungen zu — auf jedem Gerät und von jedem Standort aus. Herkömmliche Ansätze, die sich auf VPNs und Firewalls stützen, um den Anwendungszugriff zu kontrollieren, sind in einer Cloud- und Mobile-first-Welt nicht mehr effektiv genug.

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

Vorteile:

- **Mehr Produktivität bei hybriden Arbeitsmodellen** dank schnellem, nahtlosen Zugriff auf private Anwendungen unabhängig vom Userstandort
- **Minimierung des Risikos einer Datenpanne** Reduzieren Sie die Angriffsfläche und laterale Bewegungen, indem Sie Anwendungen vor dem Internet verbergen und gleichzeitig Zugriff mit minimaler Rechtevergabe erzwingen.
- **Abwehr der raffiniertesten Angreifer** Erstklassiger Schutz privater Anwendungen und vollständige Inline-Überprüfung des Traffics minimieren das Risiko kompromittierter User und aktiver Angreifer.
- **Zero-Trust-Sicherheit für Anwendungen, Workloads und Geräte** Die weltweit umfassendste ZTNA-Plattform ermöglicht den Zugriff auf private Anwendungen, Workloads und OT-/IIoT-Geräte nach dem Prinzip der geringsten Rechtevergabe.
- **Geringere betriebliche Komplexität** Unsere cloudnative Plattform macht herkömmliche Remote-Zugriffslösungen wie VPNs überflüssig, die schwer zu skalieren, zu verwalten und zu konfigurieren sind.

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 die Remote-Mitarbeiter von heute 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 und ZTNA-Angeboten der ersten Generation auf private Anwendungen 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 der nächsten Generation neu definiert werden.

Zscaler Private Access™ (ZPA)

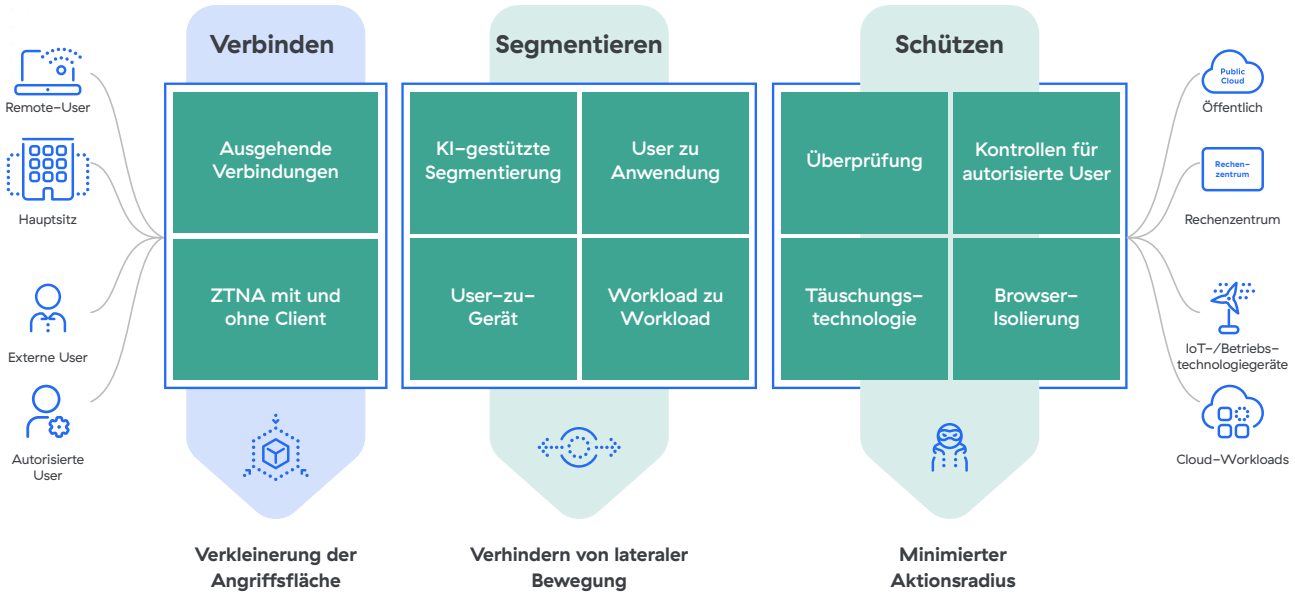
ZPA ist die weltweit am häufigsten eingesetzte ZTNA-Plattform und funktioniert nach dem Prinzip der minimalen Rechtevergabe. So können User sicher und direkt auf private Anwendungen zugreifen, die On-Premise oder in der öffentlichen Cloud ausgeführt werden, während unbefugte Zugriffe und laterale Bewegungen verhindert werden. Als cloudnativer 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:

- **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.
- **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
- **Erkennung kompromittierter User und Geräte:** Integrierte Decoys identifizieren und entfernen bösartige User und Geräte schnell.

Bis 2025 werden mindestens 70 % der neuen Bereitstellungen von Remotezugriff überwiegend über Zero Trust Network Access (ZTNA) abgewickelt werden.

— Gartner

ZPA als Antwort auf neue Anwendungsfälle für ZTNA



Die wichtigsten Anwendungsfälle

Alternative zu VPNs
VPNs wurden nicht unter Berücksichtigung von Sicherheit, Skalierbarkeit und User Experience entwickelt. Bei herkömmlichen VPNs wird der gesamte Traffic der Remote-User an Rechenzentren übermittelt, die Tausende von Kilometern entfernt sein können, was zu Latenz und Frustration bei den Usern führt. Sobald die Verbindung hergestellt ist, tunneln VPNs die User an der Firewall vorbei und platzieren sie im selben Netzwerk wie Ihre Anwendungen, was ungehinderte laterale Bewegungen ermöglicht.

ZPA bewältigt diese Herausforderungen, indem die Lösung schnellen, direkten Zugriff auf Anwendungen über mehr als 150 weltweit verteilte Points of Presence (PoPs) ohne die mit VPN verbundenen Sicherheitsrisiken bietet. Dank der Inside-Out-Konnektivität erfolgt der Anwendungszugriff unabhängig vom Netzwerkzugriff und es entsteht kein digitaler Fußabdruck. ZPA verbindet User mit Anwendungen, nicht mit Netzwerken, und User können nur auf ausgewählte Anwendungen zugreifen — ohne die Möglichkeit, sich lateral zu bewegen.

Das cloudnative 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.

Sicherheit für hybride Mitarbeiter
In der modernen Arbeitswelt sind User im Homeoffice und an anderen Remote-Standorten, in Zweigstellen und in der Zentrale tätig, was herkömmliche Sicherheitsparadigmen auf die Probe stellt. ZPA ermöglicht den nahtlosen und sicheren Zugriff auf private Anwendungen — überall und mit jedem Gerät. User im Büro profitieren durch ZPA Private Service Edge von einer identischen Erfahrung.

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. ZPA bietet jetzt universelle ZTNA-Funktionen für eine schnelle und konsistente User Experience. Darüber hinaus erhalten Sie durch Digital Experience Monitoring Echtzeiteinblicke in

Leistungseinbußen und Ausfälle, was produktives hybrides Arbeiten ermöglicht. Da ZPA Teil der Zscaler Zero Trust Exchange™ ist, profitieren User von einer integrierten SSE-Plattform für einen sicheren, schnellen und direkten Zugriff auf Internet, SaaS, Workloads, Geräte und private Anwendungen.

Zugriff für externe User/VDI-Alternative
In der Vergangenheit beruhte der Zugriff für externe User auf einer komplizierten und kostspieligen virtuellen Desktop-Infrastruktur (VDI) oder anderen Remote-Desktop-Clients wie RDP, SSH oder VNC, die User direkt mit dem Netzwerk verbanden und interne Systeme für nicht vertrauenswürdige Geräte zugänglich machten. Die Clientless-Access-Funktionen von ZPA machen den Zugriff für externe User so einfach wie den Zugriff auf das Internet und senken gleichzeitig die Kosten und minimieren die Risiken. Ihre Lieferanten, Auftragnehmer und Partner können jeden beliebigen Webbrowser auf ihren eigenen Geräten verwenden, um auf Intranet-Websites, interne Systeme und Geräte zuzugreifen — ein Client ist nicht erforderlich. Externe User und nicht verwaltete Geräte werden von Ihrem Netzwerk und Ihren Anwendungen isoliert. So wird sichergestellt, dass sensible Daten stets unter Ihrer Kontrolle bleiben und nicht ungewollt kopiert/eingefügt, gedruckt oder hoch-/heruntergeladen werden können. Mit Clientless Access kann die IT-Abteilung Usern eine bessere und sicherere Erfahrung bieten, ohne dass die Kosten für die Verwaltung der Legacy-VDI anfallen.

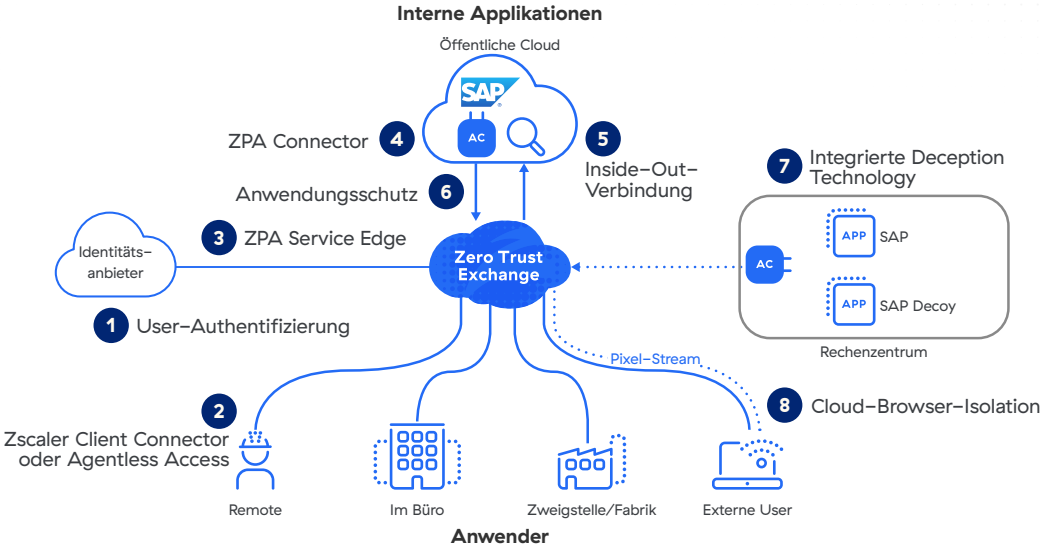
Fusionen, Übernahmen und Veräußerungen
Fusionen und Übernahmen sowie Veräußerungen erfordern häufig die Zusammenlegung von Netzwerken, was aufgrund sich überschneidender IP-Bereiche und der Einrichtung von Firewalls zwischen den beiden Unternehmen eine Herausforderung darstellen kann. ZPA beschleunigt die Integration und die Zeit bis zur Wertschöpfung nach Fusionen und Übernahmen erheblich, sodass der Prozess nur noch wenige Wochen statt Monate dauert. Die Lösung bietet nahtlosen Zugriff auf private Anwendungen — ohne VPN — und macht die Zusammenführung mehrerer Netzwerke oder die Anschaffung zusätzlicher Netzwerkgeräte überflüssig, sodass Ressourcen für wichtigere Aufgaben eingesetzt werden können.

Sicherer Bedienerzugriff für 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.

Sichere Workload-to-Workload-Konnektivität
Moderne Unternehmen benötigen schnelle, sichere Workload-to-Workload-Konnektivität in privaten, hybriden und Multicloud-Umgebungen. ZPA für Workloads reduziert die betriebliche Komplexität sowie die Kosten und stellt gleichzeitig Zero-Trust-basierte Konnektivität für Workloads in all diesen Umgebungen bereit. Da Workloads hinter ZPA verborgen werden, sind sie für das Internet unsichtbar und können nicht angegriffen werden.

Zero Trust Branch Connectivity
Zero Trust Branch Connectivity verbindet Zweigstellen, Fabriken und Rechenzentren sicher und ohne die Komplexität von VPNs und gewährleistet Zero-Trust-Zugriff zwischen Usern, IoT-/OT-Geräten sowie Anwendungen auf der Grundlage von Unternehmensrichtlinien. Durch die Verbindung von Usern und IoT-/OT-Geräten mit Anwendungen über die Zero Trust Exchange wird die Angriffsfläche eliminiert und die laterale Ausbreitung von Bedrohungen verhindert. Zero Trust Branch Connectivity vereinfacht die Kommunikation in Zweigstellen erheblich, denn komplexes Routing, VPNs und Firewalls entfallen und gleichzeitig werden flexible Weiterleitung und einfache Richtlinienverwaltung mit dem bewährten ZIA- und ZPA-Richtlinien-Framework ermöglicht.

ZPA erweitert das Prinzip der minimalen Zugriffsrechte auf das gesamte Unternehmen.



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. Authentifizierung des Users mit IdP mithilfe seiner vorhandenen SAML-SSO-Zugangsdaten.
2. Überprüfung des Gerätestatus eines Users mit Zscaler Client Connector, einem ressourcenschonenden Agent, der auf dem Laptop oder Mobilgerät des Users installiert ist. ZPA kann den Gerätestatus auch über Drittanbieter-Integrationen mit allen gängigen EPP/EDR/XDR-Anbietern (z. B. CrowdStrike, Microsoft Defender und SentinelOne) erfassen.
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. Im nächsten Schritt bestimmt die ZPA Service Edge die zum User nächstgelegene Anwendung und stellt eine sichere Verbindung zu einem ZPA App Connector her — einer ressourcenschonenden virtuellen Maschine, die in der Umgebung installiert ist, die Server und Anwendungen hostet.
5. Zwei ausgehende Tunnel, einer vom Client Connector auf dem Gerät, der andere vom App Connector, werden von der ZPA Service Edge zusammengeführt.
6. 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.
7. Durch die Integration von Zscaler Deception werden Zugriffsversuche kompromittierter User auf Decoy-Anwendungen erkannt und der Zugriff auf interne Ressourcen über die Zscaler Zero Trust Exchange blockiert.
8. Darüber hinaus können externe User mithilfe von integriertem browserbasiertem Zugriff oder Zscaler Browser Isolation agentenlos über nicht verwaltete Geräte auf private Anwendungen zugreifen.

Eine ZPA Service Edge kann entweder von Zscaler in der Cloud gehostet (ZPA Public Service Edge) oder On-Premise in Ihrer Infrastruktur ausgeführt werden (ZPA Private Service Edge). In beiden Fällen wird die Service Edge von Zscaler verwaltet, ohne dass Appliances erforderlich sind.

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.
Disaster Recovery	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 Anwendungen 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.
User-zu-Gerät-Segmentierung	Mit User-zu-Gerät-Segmentierung erfolgt jeglicher Zugriff auf IIoT-Geräte und Betriebstechnologie nur nach dem Prinzip der minimalen Rechtevergabe. Durch ZPA für IoT und Betriebstechnologie haben externe Anbieter und Remote-User die Möglichkeit, sich standortunabhängig mit Geräten zu verbinden.
Workload-zu-Workload-Segmentierung	Sichere Verbindungen und Kommunikation zwischen Workloads in Hybrid- und Multicloud-Umgebungen mit ZPA für Workloads.
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.
Integrierte Deception-Technologie	Erkennung und Abwehr der raffiniertesten Angreifer und Insider-Bedrohungen mit nativer Deception-Technologie für Anwendungen, einschließlich automatisierter Abriegelung kompromittierter User in der gesamten Zero Trust Exchange.
Integrierte Cloud Browser Isolation	Bieten Sie Auftragnehmern und Mitarbeitern mit BYOD-Geräten isolierten clientlosen Zugriff auf kritische Webanwendungen. Stellen Sie sicher, dass nicht verwaltete Endgeräte mit Sicherheitslücken oder Malware-Infektionen Ihr Netzwerk oder Ihre Anwendungen nicht gefährden. Setzen Sie Kontrollen hinsichtlich Datenexfiltration (Kopieren/Einfügen, Drucken, Upload/Download) durch, um den Verlust sensibler Daten zu verhindern.
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 Datenschutz	Weniger Bedrohungsrisiken dank vollständiger Inhaltsüberprüfung. Identifizieren und Kontrollieren sensibler Daten in Verbindungen zwischen Usern und Anwendungen.
Zero Trust SD-WAN	Verbinden Sie Zweigstellen, Fabriken und Rechenzentren sicher und unkompliziert ganz ohne VPN und regeln Sie den Zero-Trust-Zugriff von Usern, IoT-/OT-Geräten und Anwendungen mit Unternehmensrichtlinien.

Vorteile

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.

Verringerung von lateralen Bewegungen
Die auf minimalen Zugriffsrechten basierende Konnektivität stellt sicher, dass der Anwendungszugriff auf individueller Basis von einem autorisierten User auf ausgewählte Anwendungen gewährt wird und kein vollständiger Zugriff auf das Netzwerk erfolgt. Daher sind laterale Bewegungen zwischen Anwendungen oder innerhalb des Netzwerks unmöglich. Da ZPA nicht auf IP-Adressen basiert, entfällt die Notwendigkeit, eine komplexe Netzwerksegmentierung, Zugriffskontrolllisten, Firewall-Richtlinien oder Netzwerkadressübersetzungen einzurichten und zu verwalten. Mit den integrierten Deception-Funktionen von ZPA können Sicherheitsteams einen bösartigen User oder ein kompromittiertes Gerät, das versucht, sich lateral durch das Unternehmen zu bewegen, sofort erkennen und isolieren.

Abwehr von kompromittierten Usern, Insider-Bedrohungen und raffinierten Angreifern
Der einzigartige Schutz privater Anwendungen mit integrierter Inline-Überprüfung, Deception- und DLP-Funktionen minimiert das Risiko durch kompromittierte User und aktive Angreifer. ZPA stoppt automatisch Webangriffe mit vollständigem Schutz vor den gängigsten Techniken, einschließlich der OWASP Top 10, und umfassender Unterstützung userdefinierter Signaturen für sofortiges virtuelles Patching gegen Zero-Day-Schwachstellen. ZPA minimiert die Risiken durch externe User und BYOD mit komplett isoliertem Zugriff auf Anwendungen, der sensible Daten mithilfe der integrierten Cloud-Browser-Isolierung von nicht verwalteten Geräten abschirmt. Mithilfe der integrierten Deception-Technologie, die Decoy-Anwendungen einsetzt, können Sicherheitsteams aktive Bedrohungen im Netzwerk eindämmen, indem sie kompromittierten Usern den Zugriff auf Ressourcen verwehren.

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 Anwendungen, Ausfälle von Netzwerkpfaden oder Netzwerküberlastungen verursacht werden, proaktiv erkennen und beheben.

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

Editionen von Zscaler Private Access

	ZPA Essentials Edition	ZPA Business Edition	ZPA Transformation Edition	ZPA Unlimited Edition
Plattform-Services	Source IP Anchoring, mehrere Identitätsanbieter, LSS	(+) erweiterter RZ-Zugriff	(+) Testumgebung, Kunden-PKI	(+) Testumgebung, Kunden-PKI
User-zu-App-Segmentierung	10 Anwendungssegmente	500 Anwendungssegmente	Unbegrenzte Anzahl von Anwendungssegmenten	Unbegrenzte Anzahl von Anwendungssegmenten
App Connector	20 Paar	50 Paar	Unbegrenzte Anzahl von Paaren	Unbegrenzte Anzahl von Paaren
Lokaler ZTNA[1]	1 Pair (virtuell)	1 Private Service Edge Pair/5.000 User	1 Private Service Edge Pair/2.000 User	Erstes Private Service Edge Pair inbegriffen, weiteres Pair pro 1.000 User
Clientloser Zugriff[2]	—	✓	✓	✓
Integriertes Digital Experience Monitoring	—	Standard	Standard	Standard
Integrierte Deception-Technologie	—	Standard	Erweitert	Advanced Plus
Anwendungsschutz	—	—	✓	✓
Integrierte Isolierung	—	—	Standard	Advanced Plus
Datenschutz (private Anwendungen)	—	—	—	✓
Premium-Support	—	—	—	✓

Wichtige Unterscheidungsmerkmale

Als branchenweit einzige ZTNA-Plattform der nächsten Generation bietet Zscaler Private Access beispiellose Sicherheit mit einer unvergleichlichen Anwendererfahrung:

- **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 Anwendungen 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.
- **Integrierte Deception-Technologie:** Mithilfe der einzigen ZTNA-Lösung mit nativer Deception-Technologie für Anwendungen kann verhindert werden, dass sich Ransomware lateral bewegt und ausbreitet.
- **Clientloser Zugriff:** Nutzen Sie den browserbasierten Zugriff für externe User mit integrierten DLP-Funktionen.
- **Verbesserte Produktivität:** Sie erhalten lückenlose Transparenz über den Zugriff auf private Anwendungen, um User-Probleme zu erkennen, die die User Experience beeinträchtigen.
- **Globale Edge-Präsenz:** Profitieren Sie von unübertroffener Sicherheit und User Experience mit mehr als 150 Cloud-Edge-Standorten weltweit sowie einem optionalen lokalen Service Edge, um Zero Trust auf Ihre Zentrale auszuweiten.
- **Cloudnative 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.

[1]Die ZPA Business Edition unterstützt bis zu 5 Paar Private Service Edges, ab 50.000 Usern müssen zusätzliche Paare erworben werden. Die ZPA Transformation Edition unterstützt bis zu 10 Paar Private Service Edges, ab 50.000 Usern müssen zusätzliche Paare erworben werden. Die ZPA Unlimited Edition unterstützt bis zu 50 Paar Private Service Edges, ab 50.000 Usern müssen zusätzliche Paare erworben werden.

[2]Der clientlose Zugriff umfasst Browser Access und Remotezugriff mit minimaler Rechtevergabe (für bis zu 10 Systeme).

- **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.

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 Branch Connector
Branch Connector, der als physische und virtuelle Appliance erhältlich ist, verbessert die Anwendungsperformance, indem er Backhauling überflüssig macht und den gesamten Traffic von Zweigstellen und Rechenzentren direkt an den nächstgelegenen Zscaler Edge-Standort weiterleitet und so die Latenz verringert. Dadurch wird bidirektionale Kommunikation zwischen Usern, Servern und IoT-/OT-Geräten — auf denen Client Connector nicht installiert werden kann — und Anwendungen in jedem Netzwerk über die Zero Trust Exchange möglich.

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.

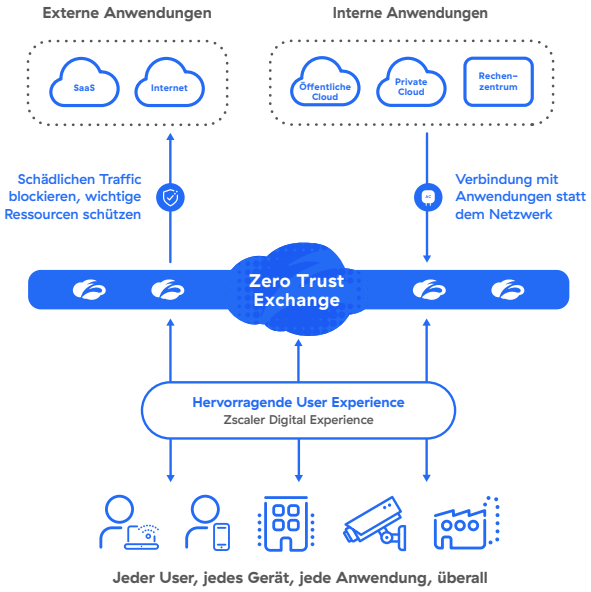
ZPA Service Edges
Service Edges setzen Sicherheits- und Zugriffsrichtlinien durch und stellen die Inside-Out-Verbindung zwischen einem autorisierten User (über Client Connector und Browser Access) und einer bestimmten privaten Anwendung (über App Connector) her. Die meisten Kunden nutzen unsere Public Service Edges, die in mehr als 150 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 cloudnative 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	macOSX 10.10 oder höher
	Android 5 oder höher	CentOS 8
	Windows 7 oder höher	Ubuntu 20.04
Branch Connector	CentOS, Redhat	VMware vCenter oder vSphere Hypervisor
Clientloser Zugriff	Moderne Webbrowser:	Chrome
	(HTML-5-fähig)	Edge
		Firefox
App Connector	AWS	Microsoft Hyper-V
	Centos, Oracle und Red Hat	VMware vCenter oder vSphere Hypervisor
	Microsoft Azure	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.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