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 werden den Anforderungen einer hybriden Belegschaft und moderner Unternehmen nicht mehr gerecht.** Firewalls und VPNs schaffen große Angriffsflächen, die Angreifer gezielt ausnutzen können. Zudem platzieren sie User direkt im Netzwerk und begünstigen so die laterale Ausbreitung von Bedrohungen. Werden Zugangsdaten kompromittiert, erhalten Angreifer leicht Zugriff auf sensible Daten. Der Einsatz von VPNs für hybride Arbeitsmodelle und den Zugriff externer User erhöht das Cyberrisiko, verschlechtert die User Experience und steigert den administrativen Aufwand. Wer Usern standort- und geräteunabhängig sicheren Zugriff bereitstellen möchte, benötigt daher einen deutlich effektiveren Ansatz.

Der Report zu VPN-Risiken 2025 von Zscaler ThreatLabz zeigt: 92 % der Befragten sehen ungepatchte VPN-Sicherheitslücken als direkten Auslöser für Ransomware-Angriffe. Das unterstreicht, wie schwierig es ist, VPNs kontinuierlich und rechtzeitig zu patchen.

### Vorteile:

- **Ersatz für angreifbare VPN-Lösungen**
  Reduzieren Sie die Angriffsfläche und unterbinden Sie laterale Bewegungen, indem Sie User direkt mit Anwendungen verbinden — nicht mit dem Netzwerk. So verbessern Sie auch Ihren Sicherheitsstatus.
- **Verhindern von Cyberangriffen**
  Minimieren Sie das Risiko von Sicherheitsvorfällen durch Schutz privater Anwendungen vor Web- und Identitätsbedrohungen sowie durch erweiterten Bedrohungsschutz mit vollständiger Inline-Überprüfung und DLP-Funktionen.
- **Schutz für hybride Belegschaften**
  Der blitzschnelle, sichere Zugriff auf private Anwendungen erstreckt sich nahtlos auf User, die Zentrale, Zweigstellen und externe User.
- **Weniger betriebliche Komplexität**
  Bieten Sie sicheren, optimierten Zugriff ohne kostspielige und komplexe Einzelprodukte über eine einheitliche, Cloud-native ZTNA-Plattform für User, Workloads und IT/OT.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

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 bremsen Skalierung und User Experience aus:** VPNs setzen auf Backhauling — das treibt Kosten und Komplexität in die Höhe und sorgt für zu hohe Latenzen für moderne Remote-Arbeitsmodelle.
- **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 einer ZTNA-Lösung (Zero Trust Network Access) 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.

**92 % der Befragten sehen ungepatchte VPN-Sicherheitslücken als direkten Auslöser für Ransomware-Angriffe. Das unterstreicht, wie schwierig es ist, VPNs kontinuierlich und rechtzeitig zu patchen.**

**— Report zu VPN-Risiken 2025 von Zscaler ThreatLabz**

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

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

## Die wichtigsten Anwendungsfälle

**Sicherer Remotezugriff (VPN-Ersatz)**
Ob aus der Cloud oder als Appliance, VPNs lassen zu viele Angriffsmöglichkeiten offen. Sie sind voller Schwachstellen, werden regelmäßig kompromittiert und vergrößern durch Backhauling und netzwerkzentrierte Architektur die Angriffsfläche. Indem User direkt ins Netzwerk eingebunden werden, begünstigen sie laterale Bewegungen — oft der Einstiegspunkt für Ransomware. Hinzu kommen schlechte Performance und hoher Verwaltungsaufwand.

Mit ZPA erhalten alle User Zero-Trust-Zugriff mit direkter Konnektivität zu privaten Anwendungen — ganz ohne Netzwerkfreigabe. Anwendungen bleiben hinter der Zero Trust Exchange verborgen, wodurch die Angriffsfläche deutlich schrumpft. KI-gestützte User-to-App-Segmentierung verhindert laterale Bewegungen, und integrierte Traffic-Überprüfung sowie Anwendungs- und Datenschutz schützen selbst vor komplexen Angriffen. ZPA bietet schnellen, direkten Zugriff auf

Anwendungen über mehr als 160 weltweit verteilte Points of Presence (PoPs) ohne die mit VPN verbundenen Sicherheitsrisiken. 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 keine zusätzliche Infrastruktur wie Anwendungskonnektoren bereitgestellt werden müssen.

**Sicherer Anwendungszugriff für Mitarbeitende im Büro und Remote-User**
Mitarbeitende arbeiten heute flexibel: im Homeoffice, in Zweigstellen oder in der Zentrale. Das sprengt die Grenzen klassischer Sicherheitsansätze. Gefragt ist nahtloser Zugriff auf Anwendungen, der auch in Krisensituationen oder bei eingeschränkter Infrastruktur Zero-Trust-Sicherheit gewährleistet. Gleichzeitig müssen Unternehmen Compliance- und regulatorische Vorgaben erfüllen, um ihre Business Continuity sicherzustellen.

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 Zugriff für externe User**
Traditionell basierte der Zugriff für externe User auf teuren, komplexen und riskanten Lösungen wie VDI, RDP, SSH oder VNC. Diese platzieren User direkt im Netzwerk und machen interne Systeme für nicht vertrauenswürdige Geräte angreifbar.

Die Clientless-Access-Funktionen von ZPA ermöglichen mühelosen Zugriff für externe User, senken Kosten und minimieren Risiken. Externe User 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. Diese User und nicht verwaltete Geräte werden so 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 Informationen zum Sicherheitsstatus in ZPA-Richtlinienüberprüfungen. Mit Clientless Access kann die IT Usern ein besseres und sicheres 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.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

**Remote-Zugriff für User mit erhöhten Berechtigungen in OT/IT-Umgebungen**
Um Ausfallzeiten zu vermeiden und die Produktion stabil zu halten, benötigen OT/IT-Teams und externe Partner regelmäßigen Zugriff auf kritische Systeme. ZPA stellt schnellen, sicheren und zuverlässigen Zugriff auf OT/IT-Umgebungen bereit — direkt am Einsatzort, am Werksgelände und an jedem anderen Standort. Mit ZPA für OT/IT erhalten User isolierten, clientlosen Remote-Desktop-Zugriff auf RDP-, SSH- und VNC-Systeme — ganz ohne Jump Hosts, Legacy-VPNs oder lokale Client-Installationen.

**Alternative zu VDI**
Fehlende Kontrolle über nicht verwaltete Geräte stellt für IT- und Sicherheitsteams ein wachsendes Risiko dar. Um dennoch Anwendungszugriff zu ermöglichen, griffen Unternehmen lange auf VDI zurück. Doch VDI platziert User direkt im Netzwerk, macht interne Anwendungen für nicht verwaltete Endgeräte erreichbar und ist zugleich teuer, komplex und kaum skalierbar. Moderne, im Rahmen der digitalen Transformation entstandene Anwendungen sind überwiegend webbasiert — ein kompletter Desktop-Stream per VDI passt nicht mehr zu den Erwartungen an eine gute User Experience.

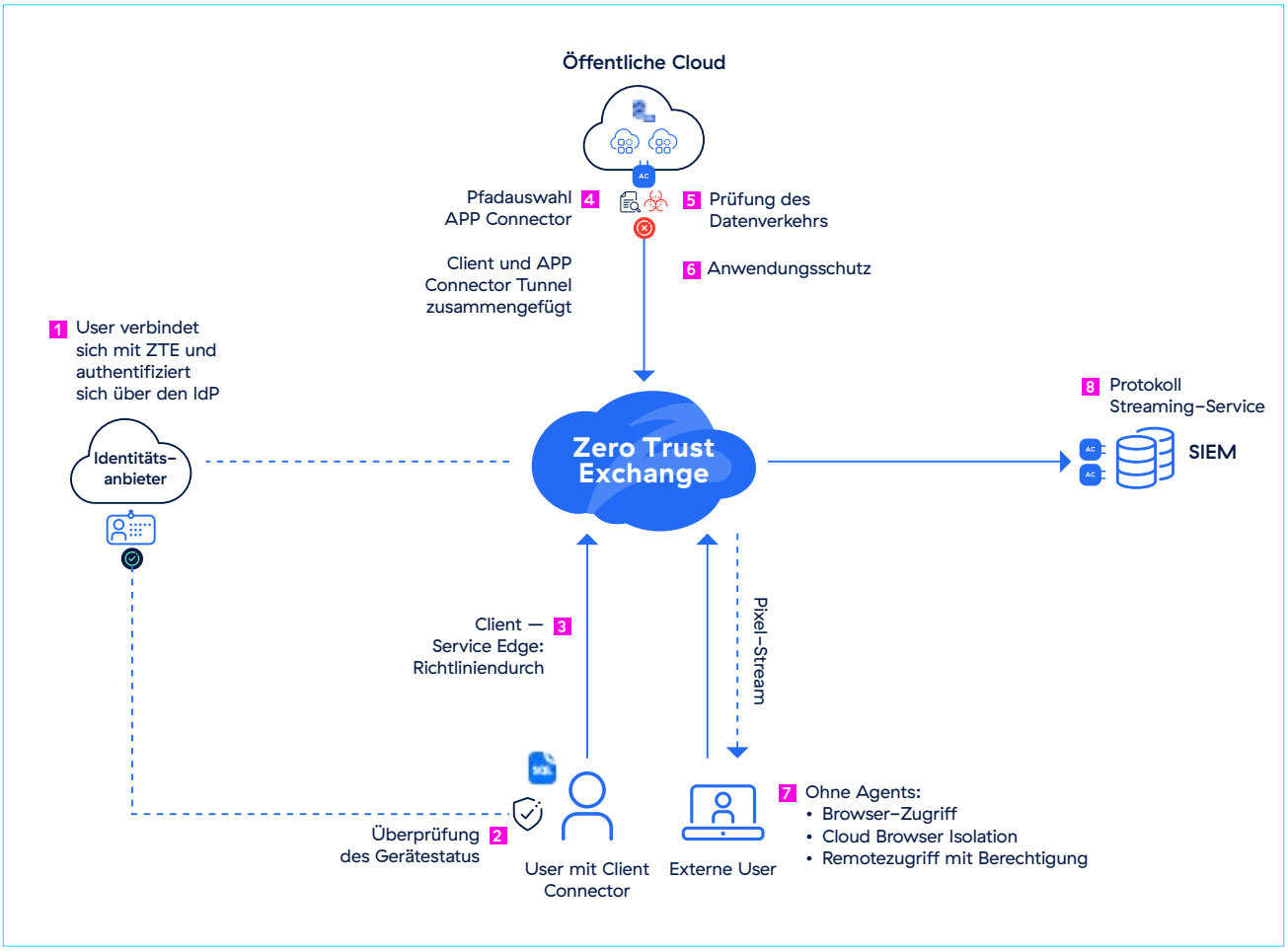
ZPA ist eine effektive VDI-Alternative, die sicheren, agentlosen, browserbasierten Zugriff auf nicht verwaltete Geräte bietet. User erhalten schnellen und nahtlosen Zugriff auf private Unternehmensanwendungen über die nächstgelegene Service-Edge. Die ZPA-Architektur bietet Direktzugriff auf Anwendungen,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

**Mikrosegmentierung (User-to-App-Segmentierung)**
Remote-Zugriffslösungen wie VPNs gewähren vollständigen Netzwerkzugriff und setzen IP-Adressen sowie Anwendungen dem Internet aus. Durch die Ausdehnung des internen Netzwerks auf externe Geräte und die Notwendigkeit von eingehendem Traffic entsteht ein öffentlich zugänglicher Angriffsvektor. Ohne angemessene Segmentierung kann ein einzelner Sicherheitsvorfall das komplette Netzwerk gefährden. Klassische Segmentierungslösungen stoßen jedoch schnell an ihre Grenzen: Firewall-Regeln werden komplex, schwer zu warten und störungsanfällig. Für große Organisationen bedeutet das zusätzlichen Aufwand durch komplexes Routing, Hochverfügbarkeitskonzepte und kostspielige private Verbindungen.

Zscaler Autonomous User-to-App Segmentation bietet eine präzise User-to-App-Segmentierung und eine robuste Lösung für die einfache Bereitstellung konsistenter Richtlinien im großen Maßstab und die Verhinderung lateraler Bedrohungsbewegungen. Sie automatisiert den gesamten Segmentierungszyklus: Anwendungen werden automatisch erkannt, mithilfe KI-gestützter Empfehlungen schneller segmentiert und der Sicherheitsstatus durch kontinuierliche Echtzeit-Einblicke nachhaltig gestärkt.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

## 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.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

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

| | |
|---|---|
| **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. |
| **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. |
| **Autonome User-to-App-Segmentierung** | Automatisieren Sie den gesamten Segmentierungszyklus: Anwendungen werden automatisch erkannt, mithilfe KI-gestützter Empfehlungen schneller segmentiert und der Sicherheitsstatus durch kontinuierliche Echtzeit-Einblicke nachhaltig gestärkt. Dank ML-gestützter Modelle, die kontinuierlich mit Millionen von Kundensignalen und Ihren individuellen Anwendungszugriffsmustern trainiert werden, unterbindet autonome User-to-App-Segmentierung die laterale Ausbreitung von Bedrohungen, beschleunigt die ZTNA-Einführung und vereinfacht Ihren Weg zu Zero Trust. |
| **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. |
| **Schutz vor Bedrohungen und Data Protection** | Weniger Bedrohungsrisiken dank vollständiger Inhaltsüberprüfung. Identifizieren und Kontrollieren sensibler Daten in Verbindungen zwischen Usern und Anwendungen. |
| **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. |
| **Sicherer Zugriff auf ältere S2C-Anwendungen** | Sichert den Zugriff auf bestehende Netzwerkanwendungen, darunter VoIP, Follow-me-Drucker und weitere Server-zu-Client-Anwendungen ab. |
| **B2B-Anwendungszugriff** | Bietet sicheren, bidirektionalen Zugriff auf Anwendungen und Workloads innerhalb des Netzwerks Ihrer Geschäftspartner (Extranet). |

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

| | |
|---|---|
| **Clientbasierter und clientloser Zugriff** | 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 schlanken Agent, dem Zscaler Client Connector. Die clientlose Option gewährleistet reibungslosen Zugriff für externe Auftragnehmer und BYOD-User unabhängig vom verwendeten Gerät und Webbrowser. |
| **ZTNA im Büro** | Setzen Sie ZTNA für User im Büro über ZPA Private Service Edges durch und gewährleisten Sie schnellen sowie nahtlosen Zugriff auf Anwendungen. 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 Krisensituationen, mit einer vom Kunden gehosteten Business-Continuity-Lösung. |

## Geschäftsnutzen

**Minimierung der Angriffsfläche**
Wenn anfällige VPNs entfallen und Anwendungen im Internet unsichtbar werden, haben Angreifer keine Angriffsfläche mehr. ZPA verbindet autorisierte User ausschließlich mit den Anwendungen, die sie benötigen — über eine isolierte Verbindung von User zu App. Dabei gibt es keinerlei eingehende Verbindungen, stattdessen entstehen verschlüsselte Mikrotunnel für ausgehenden Traffic. Über die Anwendungserkennung können Administratoren zudem unerwünschte Anwendungen, Services und Workloads automatisch identifizieren und segmentieren, wodurch sich die Angriffsfläche weiter reduziert.

**Unterbindung lateraler Bewegungen**
Konnektivität nach dem Prinzip der minimalen Rechtevergabe stellt sicher, dass Zugriffe nur isoliert von einem autorisierten User auf eine klar definierten Anwendung erfolgen — nicht auf das gesamte Netzwerk. Laterale Bewegungen zwischen Anwendungen oder im Netzwerk sind damit ausgeschlossen. Da ZPA nicht auf IP-Adressen basiert, entfällt der Aufwand für die Einrichtung und Pflege komplexer Netzwerksegmentierungen, Access Control Lists (ACLs), Firewall-Richtlinien oder Netzwerkadressübersetzungen.

**Schutz vor kompromittierten Usern, Insider-Bedrohungen und komplexen Angriffen**
Dank integrierter Inline-Überprüfung und DLP-Funktionen erkennt und stoppt ZPA kompromittierte User, Insider-Bedrohungen und aktive Angreifer frühzeitig. Webangriffe werden automatisch abgewehrt — inklusive vollständiger Abdeckung der OWASP Top 10 sowie individueller Signaturen für sofortiges virtuelles Patchen bei Zero-Day-Schwachstellen. Gleichzeitig reduziert vollständig isolierter Anwendungszugriff die Risiken durch externe User und BYOD und verhindert mithilfe von integrierter Cloud-Browser-Isolierung, dass sensible Daten auf nicht verwaltete Geräte gelangen.

**Erstklassige User Experience**
Durchgängig schnelle Verbindungen ohne ständiges An- und Abmelden bei VPN-Clients sorgen für sicheren und effizienten Remote-Zugriff. Externe Dienstleister, Lieferanten und Partner erhalten reibungslosen Zugriff von jedem Gerät und über jeden Webbrowser — ganz ohne Client-Installation. Die Anmeldung erfolgt bequem über bestehende SSO-Zugangsdaten wie Azure AD, Okta oder Ping. Gleichzeitig behalten Administratoren die Kontrolle und erkennen Performanceprobleme frühzeitig, um Produktivitätseinbußen durch Zugriffsprobleme, Netzwerkausfälle oder Engpässe zu vermeiden.

**Eine einheitliche Plattform für sicheren Anwendungs-, Workload- und Gerätezugriff**
Erweitern Sie Zero Trust auf private Anwendungen sowie OT- und IT-Geräte, um bislang getrennte Remotezugriffstools zu konsolidieren. So vereinheitlichen Sie Sicherheits- und Zugriffsrichtlinien, verhindern Sicherheitsvorfälle und reduzieren die operative Komplexität.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

## Zscaler Private Access (ZPA): Mehrere Optionen für den Einstieg

| | Zscaler-Essentials-Plattform (ZS-ESS-PLATFORM) | ZPA Clientless Platform (ZPA-CLIENTLESS-PLATFORM) | Zscaler-Private-Access-Plattform (ZS-ZPA-PLATFORM) | Zscaler-Plattform (ZS-PLATTFORM) |
|---|---|---|---|---|
| Private Access Platform Services | | | | |
| Granulare Zugriffskontrolle nach User, Gruppe und Ports | ✓ 1 User pro 20 Abonnenten (Min.: 500 Abonnenten) | ✓ | ✓ | ✓ |
| Protokoll Streaming-Service | | | | |
| Permanente Zustandsüberwachung für alle Applikationen | | | | |
| Quell-IP-Verankerung: Selektive Weiterleitung des Anwendungstraffics an die entsprechenden Zielserver | | | | |
| App Connector: Schlanke VM, die ausgehende Verbindungen zur Zscaler ZTE ermöglicht | So viele wie erforderlich (bis zur max. Anz. für das System) | So viele wie erforderlich (bis zur max. Anz. für das System) | So viele wie erforderlich (bis zur max. Anz. für das System) | So viele wie erforderlich (bis zur max. Anz. für das System) |
| ZPA Private Service Edge: ZTNA für Remote- und Büro-User | – | – | | |
| ZPA für Legacy-Anwendungen (VOIP, S2C usw.) | – | – | Add-on: VPN Service Edges (mind. 50 User) | Add-on: VPN Service Edges (mind. 50 User) |
| ZPA Business Continuity Cloud | – | – | Add-on (mind. 500 User) | Add-on (mind. 500 User) |
| User-to-App-Segmentierung | 10 Anwendungssegmente | 20 Anwendungssegmente | 20 Anwendungssegmente | 20 Anwendungssegmente |
| Autonome User-to-App-Segmentierung und Insights | – | – | **ADD-ON** | **ADD-ON** |
| Zugang von Drittparteien | | | Add-on (mind. 500 User) | Add-on (mind. 500 User) |
| Browserbasierter Zugriff für nicht verwaltete Geräte | – | ✓ | ✓ Zusätzliche Lizenzen für Gastuser können mit ZPA-CLIENTLESS-PLATFORM erworben werden. | ✓ Zusätzliche Lizenzen für Gastuser können mit ZPA-CLIENTLESS-PLATFORM erworben werden. |
| Userportal: Zentrales Webportal, über das User auf autorisierte Anwendungen und privilegierte Konsolen zugreifen können | | | | |
| Privileged Remote Access Standard: Clientloser PRA für OT-Systeme (bis zu 10 Systeme) (RDP/SSH/VNC) | | | | |
| Browser Isolation für private/ SaaS-Anwendungen | | **ADD-ON** | **ADD-ON** | **ADD-ON** |
| Digital Experience Monitoring | – | – | ✓ | ✓ |
| ZDX Standard: Einblicke in User-, Verbindungs- und Anwendungstelemetrie | | | | |
| Schutz für private Anwendungen und Daten | **ADD-ON** | | | |
| Datenschutz für private Anwendungen, Incident Response und Datenklassifizierung | | – | **ADD-ON** | ✓ |
| Zscaler Deception: Integrierte Köder zur Erkennung kompromittierter User | | – | ✓ (Mind. 500 User) | ✓ (Mind. 500 User) |
| AppProtection schützt private Awendungen vor den OWASP Top 10 und überprüft Web-Traffic | | **ADD-ON** | **ADD-ON** | **ADD-ON** |

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

## 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 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.
- **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.
- **Sicherer Browserzugriff:** Nutzen Sie browserbasierten Zugriff für externe User mit integrierten DLP-Funktionen.
- **Unterbindung lateraler Bewegungen durch autonome User-to-App-Segmentierung:** Bietet präzise User-to-App-Segmentierung, schafft Transparenz über Zugriffe und optimiert Richtlinien mithilfe von Machine Learning, um die Angriffsfläche zu minimieren und die laterale Ausbreitung von 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.

Gartner

Zscaler wurde als Leader im Gartner® Magic Quadrant™ für Security Service Edge 2025 ausgezeichnet**

Mehr erfahren

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

## Grundlegende Komponenten

**Zscaler Client Connector**
Client Connector ist eine schlanke Anwendung für Laptops und Mobilgeräte. Er leitet den Traffic automatisch an die nächstgelegene Zscaler Service Edge weiter und stellt so sicher, dass Sicherheits- und Zugriffsrichtlinien geräte-, standort- und anwendungsübergreifend durchgesetzt werden.

**Zscaler Clientless Access**
Sicherer Zugriff auf Anwendungen, Workloads und OT-Geräte ist sowohl über integrierten Browserzugriff (Web, RDP, SSH, VNC) als auch über Zscaler Browser Isolation möglich — ganz ohne Client, selbst auf nicht verwalteten Geräten.

**ZPA App Connector**
App Connectors sind schlanke virtuelle Maschinen, die vor privaten Anwendungen im Rechenzentrum oder in der öffentlichen Cloud platziert werden. Sie vermitteln sichere Verbindungen zwischen autorisierten Usern und klar definierten Anwendungen über eine ausgehende Verbindung, die Anwendungen vollständig vor dem Internet verbirgt.

**ZPA Network Connector**
Network Connectors sind schlanke virtuelle Maschinen, die vor den Anwendungsservern im Rechenzentrum bereitgestellt werden. Sie verbinden sich über einen ausgehenden Tunnel mit den VPN Service Edges in der Zscaler Cloud.

**ZPA Service Edges**
Service Edges setzen Sicherheits- und Zugriffsrichtlinien durch und verbinden autorisierte User (über Client Connector und Browser Access) mit einer spezifischen privaten Anwendung (über App Connector). Die meisten Kunden nutzen unsere Public Service Edges, die an über 160 Points of Presence (PoPs) weltweit betrieben werden und Millionen gleichzeitiger User der größten Unternehmen der Welt unterstützen. Private Service Edges, die von Zscaler verwaltet werden, können auch vor Ort gehostet werden, um lokalen Usern den kürzesten Weg zu On-Premise-Anwendungen zu bieten, ohne das lokale Netzwerk zu verlassen. Gleichzeitig wird die Business Continuity sichergestellt, da selbst in unvorhersehbaren Krisensituationen auf geschäftskritische Anwendungen zugegriffen werden kann.

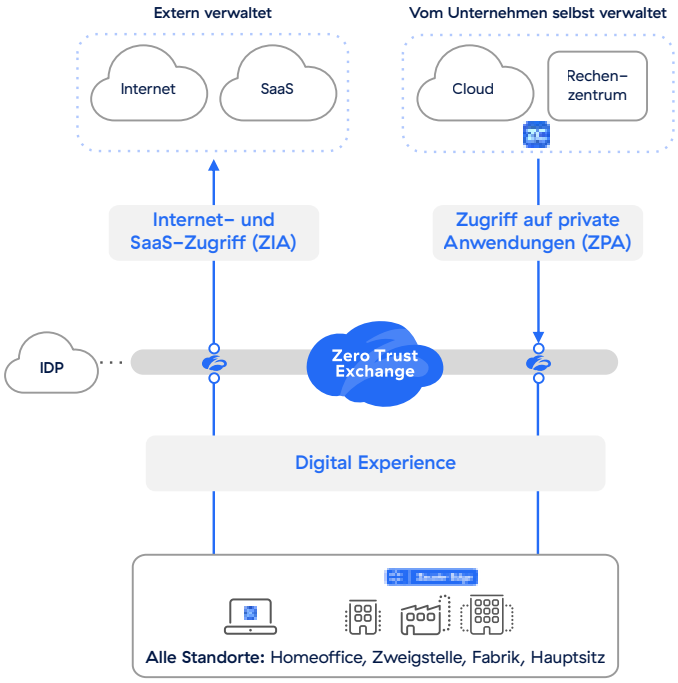
**ZPA Private Cloud Controller**
Private Cloud Controllers fungieren als mandantenbezogene Steuerinstanz für User, ZPA Private Service Edges und App Connectors, um auch dann nahtlosen Zugriff zu ermöglichen, wenn die Zscaler Cloud nicht erreichbar ist.

## 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.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

## Zscaler schützt Ihre Mitarbeiter: Sicherer, schneller und zuverlässiger Anwendungszugriff — innerhalb weniger Tage einsatzbereit für mehr Cybersicherheit und eine optimierte User Experience




Hervorragende Anwendererfahrung, überlegener Bedrohungsschutz und Data Protection, weniger Kosten und Komplexität

## Technische Spezifikationen

| Zscaler-Komponente | Unterstützte Plattformen und Systeme | |
|---|---|---|
| **Client Connector** | iOS 17 oder höher<br>Android 9 oder höher<br>Windows 8 oder höher | ChromeOS Version 137 oder höher<br>Linux<br>MacOS 14 oder höher |
| **Clientloser Zugriff** | Moderne Webbrowser (HTML5-fähig): Chrome, Edge, Firefox, Safari | |
| **App Connector** | AWS, GCP, Microsoft Azure, Nutanix, VMware, OpenShift, Docker, Red Hat | |
| **Private Service Edge** | AWS, GCP, Microsoft Azure, Nutanix, VMware, Docker, Red Hat | |
| **Private Cloud Controller** | AWS, Microsoft Azure, VMware, Red Hat | |

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 SSE-basierte Zero Trust Exchange ist auf über 150 Rechenzentren der ganzen Welt verteilt und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf **zscaler.com/de** oder folgen Sie uns auf Twitter unter **@zscaler**.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ und weitere unter **zscaler.com.de/legal/trademarks** aufgeführte Marken sind entweder (i) eingetragene Marken bzw. Dienstleistungsmarken oder (ii) Marken bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.

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