Die Cloud-Herausforderung: schnell und sicher expandieren

Erweitern Sie den Zero-Trust-Schutz auf Ihre gesamte AWS-Cloud-Umgebung.



E-BOOK

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

Inhaltsverzeichnis



Die Cloud-Herausforderung: schnell und sicher expandieren 3

Die zukunftsfähige Cloud-First-Lösung von Zscaler 4

ZPA: eine nahtlose Cloud-First-Lösung für Zero-Trust-Zugriff auf private Unternehmensanwendungen 5

Zero Trust Cloud: eine überlegene Sicherheitslösung für Cloud-Workloads 6

ZDX: schnelle, nahtlose Anwendererfahrungen für Enduser 7

Eine gemeinsame Lösung mit einfacher und schneller Bereitstellung 8

Die Transformation der Cloud-Sicherheit: Ist Ihr Unternehmen bereit? 9

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

Die Cloud-Herausforderung: schnell und sicher expandieren

Herkömmliche netzwerkbasierte Zugriffskontrollen wie VPNs sind für heutige Cloud-Umgebungen nicht optimal. Welche alternativen Lösungswege gibt es demnach?

Mehr als 94—96 %[1] aller Unternehmen weltweit nutzen Cloud-Services, wobei auf AWS mittlerweile ein Anteil von 30 %[2] am globalen Cloud-Infrastruktur-Markt entfällt. Die Vorteile der Cloud-Nutzung sind unbestreitbar — von Kosteneinsparungen bis hin zu agiler Skalierbarkeit. Unternehmen, die in der Cloud arbeiten, stehen vor zwei neuen Herausforderungen: der Verwaltung von Zugriff und Betrieb angesichts des zunehmenden Trends zu Remote- und Hybridarbeitsmodellen sowie der immer komplexeren Bedrohung durch Malware und Ransomware.

Früher erforderte die Implementierung einer sicheren Umgebung ein netzwerkzentriertes Virtual Private Network (VPN). Dabei ging die Kontrolle jedoch zulasten der Geschwindigkeit, Benutzerfreundlichkeit und Flexibilität. Da Unternehmen heutzutage vermehrt in die Cloud migrieren und der Umfang ihrer IT-Abläufe zunimmt, werden die Nachteile der Nutzung eines VPN immer deutlicher.

VPNs sind grundsätzlich nicht darauf ausgelegt, einen von Natur aus sicheren Internetzugang zu gewährleisten. Stattdessen sind Unternehmen darauf angewiesen, dass User an Remote-Standorten über eine stabile Internetverbindung verfügen und aktuelle Sicherheitsvorkehrungen anwenden. Da die Belegschaften der Unternehmen, die in die Cloud migrieren, von überall aus arbeiten, haben sich die eingehenden Verbindungen ausgeweitet, wodurch sich die Möglichkeiten für DDoS-Angriffe vergrößert haben. Dies wiederum erhöht die Komplexität der Zugriffssegmentierung angesichts der eingeschränkten Transparenz über die Aktivitäten der User im Netzwerk. Letztendlich schränken diese Hürden die Skalierbarkeit ein, erhöhen die Kosten, behindern die Produktivität und beeinträchtigen die Qualität der User Experience für die Mitarbeitenden. In einigen Fällen hat dies auch Auswirkungen auf den Enduser — den Kunden.

Um hier Abhilfe zu schaffen, arbeitet AWS mit Zscaler zusammen, einer führenden Zero-Trust-Plattform, die die Netzwerk- und Sicherheitsbranche revolutioniert. Als AWS Advanced Technology Partner bietet Zscaler Security-as-a-Service auf Basis eines Zero-Trust-Modells, um Unternehmen dabei zu unterstützen, eine echte Cloud-Transformation — sicher und einfach — jetzt und in Zukunft zu erreichen.



©2026 Zscaler, Inc. Alle Rechte vorbehalten.

Zscaler in Zahlen

PRO TAG:

Über

9 Milliarden

Bedrohungen

Über

750 Milliarden

Transaktionen

Über

250

individuelle Sicherheitsupdates

Die zukunftsfähige Cloud-First-Lösung von Zscaler

Eine konfigurierbare Produktsuite für vereinfachten Zugriff und erhöhte Sicherheit, die mit Blick auf die Multicloud-Komplexität entwickelt wurde

Ganz gleich, ob ein Unternehmen Workloads in die Cloud verlagern oder sich einfach nur von einem VPN lösen möchte, das Fazit ist eindeutig: Die Kombination von Zscaler und AWS bietet erstklassige Sicherheit und eine hervorragende Anwendererfahrung mithilfe modernster Technologie und eines Zero-Trust-Modells.

Die anwendungszentrierten Sicherheitsservices von Zscaler wurden von Grund auf in der Cloud entwickelt und ersetzen die traditionellen ein- und ausgehenden Gateways durch einen moderneren Ansatz, was sich insbesondere für Unternehmen, die AWS nutzen, anbietet. Drei Kern-Services unterstützen AWS-Kunden dabei, das Beste aus ihrem Cloud-Betrieb herauszuholen:

Zscaler Private Access (ZPA) macht VPNs überflüssig, da User mit Anwendungen anstatt mit Netzwerken verbunden werden. So werden Applikationen aus dem Internet entfernt, was durch einfachere Verwaltung der Tools und Vorgänge hinter den Kulissen, mit denen User nicht interagieren, zu einer sichereren Umgebung und einer geringeren Backend-Komplexität führt.

Zscaler Zero Trust Cloud (ZTC) zentralisiert und standardisiert das Workload-Sicherheitsmanagement in allen Cloud-Umgebungen durch ein einziges, konsistentes Framework und ermöglicht so eine identitätsbasierte Segmentierung, einheitliche Richtliniendurchsetzung und einheitliche Transparenz in hybriden und Multi-Cloud-Umgebungen.

Zscaler Digital Experience Monitoring (ZDX) ist eine mandantenfähige Cloud-basierte Monitoring-Plattform, die digitale Anwendererfahrungen für alle User innerhalb eines Unternehmens prüft, bewertet und misst.

Gemeinsam unterstützen Zscaler und AWS Organisationen dabei, Unternehmen optimal für die Zukunft aufzustellen. Erreicht wird dies durch:

- einen ununterbrochenen Zugriff zur Verbesserung der Anwendererfahrung;
- effizienteres Routing für geringere Latenz und eine kürzere Zeit zur Produktion;
- einen stärkeren, umfassenderen Sicherheitsstatus zur Beseitigung von Bedrohungen;
- eine schnellere Migration von Applikationen für minimale Ausfallzeiten;
- eine erhöhte Geschäftsagilität zur Steigerung des Wettbewerbsvorteils;
- geringere Kosten und damit die Freisetzung finanzieller Mittel, die anderweitig im Unternehmen besser eingesetzt werden können.

Diese Tools können zwar jedem Unternehmen dabei helfen, zukunftsfähig zu werden, aber sie erweisen sich als besonders wertvoll, wenn es um kritische Anwendungsfälle geht. Mit Zscaler lassen sich beispielsweise viele der technischen Probleme beseitigen, mit denen sich IT-Fachkräfte bei Fusionen und Übernahmen konfrontiert sehen. Durch eine deutlich geringere Komplexität des Integrationsprozesses sowie die Einhaltung von Best Practices im Bereich Sicherheit hat Zscaler Unternehmen dabei geholfen, technische Einrichtungsprozesse von Monaten auf Wochen zu verkürzen. Die fusionierten Unternehmen können ihre Mitarbeitenden direkt mit den Anwendungen verbinden, ohne dass es zu Problemen oder Verzögerungen bei der Erstellung oder Verlegung von Netzwerken kommt.

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

ZPA: eine nahtlose Cloud-First-Lösung für Zero-Trust-Zugriff auf private Unternehmensanwendungen

Umständliche VPNs durch reibungslosen Zugriff auf Anwendungen ersetzen, mit dem private Apps nicht ins Internet gelangen und so für externe Bedrohungsakteure unsichtbar bleiben

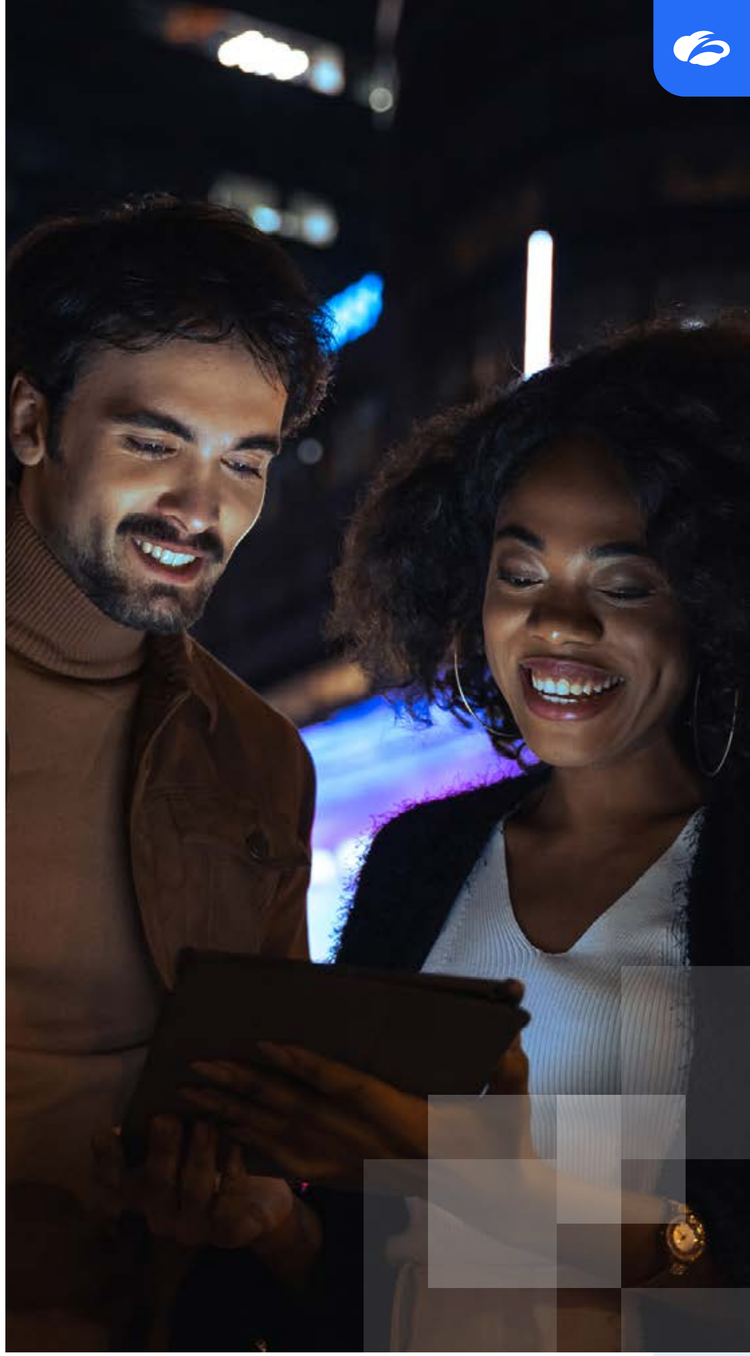
VPNs, die jahrzehntelang als beste Option für Private Access galten, sind in der Cloud-basierten Welt von heute zunehmend umständlich und anfällig: User werden in ein Netzwerk geroutet, nur um anschließend wieder hinausgeleitet zu werden. Anwendungs-Verbindungen für Remote-Mitarbeitende durchlaufen weltweit unterschiedliche Touchpoints — von Firewalls bis hin zu Load Balancern — und umfassen somit sogar noch mehr Schritte. Darüber hinaus setzt ein VPN voraus, dass der User weiß, welches Profil zu verwenden ist und welche Ressourcen den Zugriff und somit eine Verbindung zum Netzwerk ermöglichen. All dies führt zu einer suboptimalen Anwendererfahrung, insbesondere für technisch weniger versierte Mitarbeiter.

Sichere Anbindung von Zweigstellen

ZPA gewährleistet sicheren Remotezugriff auf Anwendungen ohne VPN und Netzwerkzugang und stützt sich dabei nicht auf IP-zentrierte physische oder virtuelle Appliances. Der autorisierte User-Zugriff wird vor, während und nach der Migration von Anwendungen zu AWS verwaltet. Dabei wird ein wesentlich effizienterer und sicherer Pfad verwendet: eine SDP-Lösung (Software Defined Perimeter) basierend auf Zero Trust, die eine von einem AWS App Connector in der globalen Security Cloud von Zscaler hergestellte ausgehende Verbindung nutzt — eine Lösung, die auch ergänzend zu AWS Native Security Groups und AWS Direct Connect eingesetzt werden kann. Unabhängig davon, von welchem Standort User sich mit internen Anwendungen verbinden, sorgt ZPA für eine schnellere Migration von Applikationen, geringere Kosten und ein reduziertes Bedrohungsrisiko — selbst für Unternehmen, die noch auf ein privates Rechenzentrum angewiesen sind. So werden Skalierbarkeit und Agilität perfekt miteinander vereint.

ZPA Northstar: GROWMARK sorgt für reibungslose Abläufe in der Lebensmittelproduktion

Das nordamerikanische Landwirtschaftsunternehmen GROWMARK bietet unterschiedliche Materialien und Services zur Unterstützung des Pflanzenwachstums an. Das Unternehmen beschäftigt Mitarbeitende an mehr als 500 ländlichen Standorten und ist mit den Herausforderungen unzuverlässiger Internetverbindungen bestens vertraut. Angesichts der COVID-19-Pandemie sowie der daraus resultierenden Lieferkettenprobleme war es für das Unternehmen noch wichtiger als sonst, für reibungslose Abläufe zu sorgen. Im Zuge der Modernisierungsmaßnahmen von GROWMARK verlagerte das Unternehmen Hunderte von Anwendungen zu AWS. Gleichzeitig wurden einige Applikationen vor Ort gehostet, weshalb eine Lösung benötigt wurde, die sich mit der hybriden Struktur vereinbaren ließ. Nachdem sich GROWMARK für ZPA entschieden hatte, konnte das Unternehmen seinen Mitarbeitern eine zuverlässigere Verbindung zur Verfügung stellen und gleichzeitig öffentliche Schnittstellen aus der privaten Umgebung entfernen, was letztlich zu einer Reduzierung der Angriffsfläche führte. Zum Höhepunkt der Pandemie konnten 98 % der GROWMARK-Mitarbeiter nahezu ohne Probleme eine Verbindung zu ZPA herstellen.



©2026 Zscaler, Inc. Alle Rechte vorbehalten.



Eine einheitliche Lösung für starke, skalierbare Cloud-Sicherheit

Zero Trust Cloud: eine überlegene Sicherheitslösung für Cloud-Workloads

Firewalls statt Zero Trust: Transformieren Sie Ihre Workload-Sicherheit

Unternehmen, die mit Hybrid- und Multi-Cloud-Umgebungen arbeiten, stellen fest, dass herkömmliche netzwerkzentrierte Sicherheitsmodelle für die Absicherung moderner Workloads nicht effektiv sind. Da Anwendungen und Services zwischen Rechenzentren, privaten Clouds und öffentlichen Cloud-Umgebungen verschoben werden, lassen sich herkömmliche Kontrollmechanismen, die einst zur Segmentierung und Sicherung des Datenverkehrs beitrugen, immer schwieriger verwalten und skalieren. Statische IP-basierte Regeln, inkonsistente Richtlinienmodelle und disparate Sicherheitstools erzeugen Komplexität, verringern die Transparenz und erhöhen das Risiko der lateralen Ausbreitung von Bedrohungen. Die Notwendigkeit, den lateralen sowie den ein- und ausgehenden Traffic kontinuierlich abzusichern, stellt eine zusätzliche Belastung für IT- und Sicherheitsfachkräfte dar.

Geringe Fehlertoleranz in der Cloud

Zscaler Zero Trust Cloud wendet Zero-Trust-Prinzipien an, sodass AWS-Workloads niemals implizit aufgrund ihres Netzwerkstandorts als vertrauenswürdig eingestuft werden. Dies verschafft Unternehmen einen entscheidenden Wettbewerbsvorteil im Rahmen des allgemeinen Trends zur Modernisierung der Sicherheit verteilter Anwendungen und Infrastrukturen. Mit ZTC können Unternehmen das Sicherheitsmanagement von Workloads in Hybrid- und Multi-Cloud-Umgebungen zentralisieren und standardisieren und so einheitliche Transparenz und konsistente Richtliniendurchsetzung für Workloads überall dort gewährleisten, wo sie ausgeführt werden.

ZTC Northstar: Wie FICO Produktions-Workloads in der Cloud sichert.

Das Analytics-Softwareunternehmen FICO treibt seine Cloud-Transformation voran und unterstützt gleichzeitig weiterhin Anwendungen in Rechenzentren. Da immer mehr Produktions-Workloads in die AWS-Cloud verlagert werden, benötigte das Unternehmen eine einheitliche Methode, um die Sicherheitskontrollen über Cloud-Umgebungen hinweg zu erweitern, ohne auf fragmentierte Ansätze angewiesen zu sein. Um diesen Wandel zu unterstützen, implementierte FICO Zscaler Cloud Connectors, um AWS-Konten sicher mit Zscaler-Services zu verbinden und so die gleichen Schutzmaßnahmen, die für User und den Zugriff auf private Unternehmensanwendungen gelten, auch auf Cloud-Workloads auszuweiten. Nachdem die Workloads aktuell nach Zone und AWS-Konto segmentiert sind, strebt FICO nun eine feinere Segmentierung an, um seine Cloud-Präsenz auszubauen und die Kontrolle über das Workload-Sicherheitsmanagement zu stärken.

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

ZDX: schnelle, nahtlose Anwendererfahrungen für Enduser

Tiefe, verwertbare Einblicke in die Benutzererfahrung anhand einer einheitlichen Sicht auf die Performancemetrik von Applikationen, Endgeräten und CloudPath.

In puncto Anwendererfahrung sind Verbraucher heutzutage einen extrem hohen Standard gewöhnt — selbst ein vorübergehender Social-Media-Ausfall sorgt mittlerweile für Schlagzeilen. Unternehmen waren zwar im Begriff, Probleme hinsichtlich der Anwendererfahrung mithilfe der internen Technologie vor Ort zu bewältigen, doch angesichts der durch schlechte Internetverbindungen und unterschiedliche (und teils veraltete) persönliche Mobilgeräte verursachten Probleme von Remote- und Hybrid-Teams kam es verstärkt zu Engpässen. Führt dies zu Unterbrechungen und ständigen Neuverbindungen, sammeln sich Support-Tickets an und Arbeit bleibt liegen. Dadurch gerät die IT-Abteilung unter Druck: Die Ursache (und Lösung) der spezifischen Probleme muss schnellstmöglich gefunden werden.

Reibungslose Verbdinungen für sämtliche Enduser

ZDX ist eine mandantenfähige, Cloud-basierte Monitoring-Plattform zur Prüfung, Bewertung und Messung der digitalen Anwendererfahrungen sämtlicher User innerhalb eines Unternehmens — unabhängig vom jeweiligen Standort. ZDX ermittelt in Echtzeit, wodurch ein Problem verursacht wird (z. B. durch die Internetverbindung oder den Internetdienstanbieter) und setzt daraufhin seine Remote-Fehlerbehebungsfunktionen ein. Analysen messen die Performance über einen bestimmten Zeitraum nach Standort, User und Abteilung, um Trends zu erkennen und Verbesserungen zu ermöglichen. Das Ergebnis? Eine echte SASE-Architektur (Secure Access Server Edge), die für eine bessere Anwendererfahrung und weitaus weniger IT-Tickets sorgt.

ZDX Northstar: Zufriedene User bei Liberty Mutual

Im Jahr 2020 konnte Liberty Mutual Insurance zum Leidwesen vieler zwar für seine Rechenzentren und die ISP-Bandbreite eine Gewährleistung geben, nicht aber für die Internetverbindung der Mitarbeitenden im Homeoffice. Für einen Proof of Concept konzentrierte sich das Sicherheitsteam von Liberty zunächst auf 100 User und führte ZDX als ersten Anwendungsfall für User mit Langzeitproblemen ein. So wurden Probleme an das Level-2-Helpdesk-Team weitergegeben, das die Probleme der User mit Heimnetzwerken mühelos lösen konnte. Inzwischen wurde ZDX im gesamten Unternehmen integriert, um unter anderem Latenzprobleme von Serviceanbietern, Probleme mit WLAN-Routern, Speicherlecks auf Desktop-Computern sowie ISP-Probleme im Zusammenhang mit der Seitenladezeit zu ermitteln und zu beheben.



©2026 Zscaler, Inc. Alle Rechte vorbehalten.

Eine gemeinsame Lösung mit einfacher und schneller Bereitstellung

Mit einem auf Geschwindigkeit ausgelegten Bereitstellungsprozess sowie dem Zscaler Client Connector für Zugriffsmanagement sind Teams in nur wenigen Minuten einsatzbereit.

Die Umstellung auf eine neue Plattform und IT-Infrastruktur kann komplex und langwierig sein. Um diesem Problem zu begegnen, hat Zscaler den Bereitstellungsprozess auf Geschwindigkeit und Einfachheit ausgerichtet — sichere Cloud-basierte Abläufe und reibungslose Übergänge werden mit Zscaler und AWS vereinfacht.

ZPA, ZIA, und **ZDX** können jeweils als eigenständige Einzellösungn eingesetzt werden. Für den Aufbau eines auf reibungslosen Anwendungszugriff ausgelegten Frameworks sollten sie jedoch am besten kombiniert werden. Das Herzstück ihrer Prozesse bildet der Zscaler Client Connector (ZCC).

ZPA verwendet den Client Connector, um User mithilfe eines Zero-Trust-Ansatzes mit privaten Applikationen zu verbinden, wobei für rein webbasierte private Unternehmensanwendungen auch ein Browser-Zugriff möglich ist.

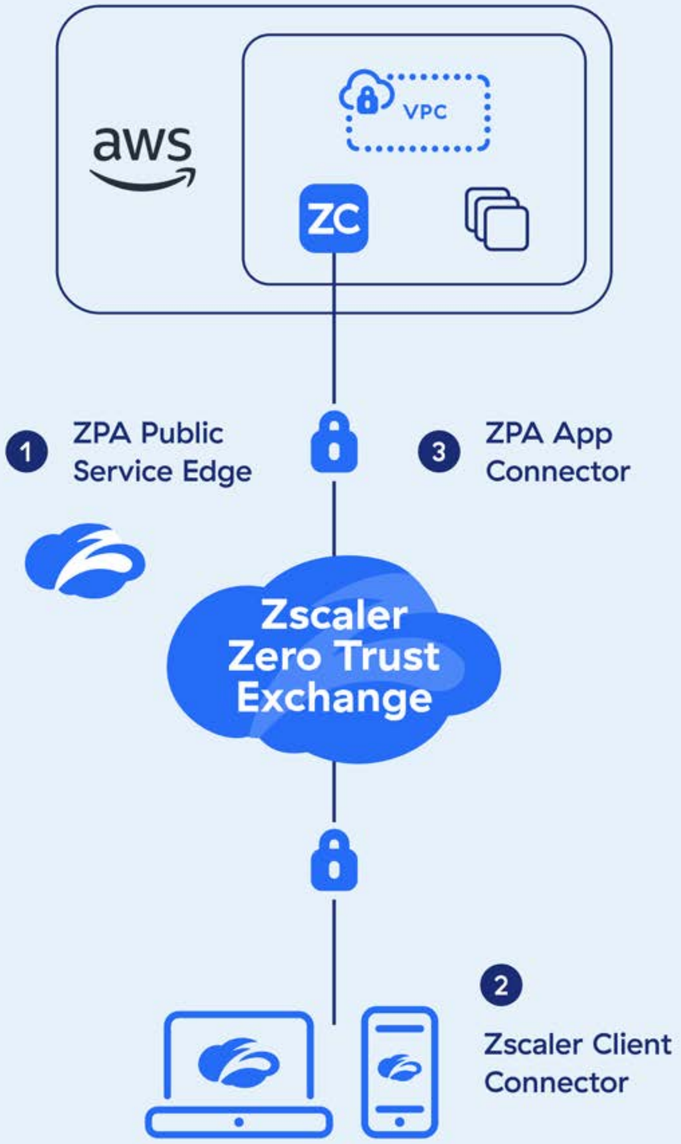
ZIA nutzt den Client Connector, um User außerhalb des Unternehmensnetzwerks zu schützen. Der Internet-Traffic wird hierbei durch den Service von Zscaler geleitet, um die Durchsetzung granularer Sicherheitsrichtlinien zu gewährleisten.

ZDX verwendet den Client Connector für synthetische Tests gewünschter SaaS-Applikation (Software-as-a-Service) oder internetbasierter Services wie z. B. Salesforce oder Zoom.

Zscaler-Kunden können VPNs schnell, sicher und endgültig ersetzen.
Hier erfahren Sie, wie das in der Praxis aussieht.

- **ZPA Public Service Edge** hostet die Richtlinien-Engine und vermittelt Verbindungen
- **Zscaler Client Connector** leitet den Traffic an die Zscaler Cloud weiter
- **ZPA App Connector** stellt Verbindungen zu privaten Unternehmensanwendungen her und erkennt neue Anwendungen. Die schnelle und reibungslose Bereitstellung von Zscaler ermöglicht eine einfache Umstellung von VPNs.
- Die IT-Abteilung installiert die Anwendungskonnektoren in AWS, sodass Zscaler die Anwendungen erreichen kann, auf die User zugreifen müssen.
- Im ZPA-Portal werden Anwendungen und Konnektoren definiert und den Servergruppen zugewiesen.
- Einmal installiert, erfüllt der Client Connector gleich mehrere Zwecke: Er ermittelt, wohin Anfragen gerichtet sind, wohin sie gehen sollen und wo User verbunden werden.

Weitere Informationen über die Konfiguration für den Client Connector



©2026 Zscaler, Inc. Alle Rechte vorbehalten.



Bereit für die Transformation der Cloud-Sicherheit?

Zscaler und AWS bieten eine überzeugende Lösung für die Herausforderungen des User-Zugriffs.

aws marketplace

Finden Sie Zscaler-Lösungen im AWS Marketplace für vereinfachte Abrechnung und Bereitstellung direkt auf AWS.

Kostenlose 7-tägige gehostete ZPA-Demo testen.

Mit nur wenigen Klicks lässt sich ein Bericht von Zscaler erstellen, der eine detaillierte Bewertung des Cloud-Sicherheitsstatus liefert und zeigt, wo die Sicherheitsrisiken von Unternehmen im Internet liegen.

Starten Sie eine Internet-Bedrohungsanalyse.

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

zscaler™

Schneller agieren.
Dauerhaft schützen.

©2026 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™ und ZPA™ sind entweder (i) eingetragene Markenzeichen bzw. Dienstleistungsmarken oder (ii) Markenzeichen bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.

aws Erhältlich im AWS Marketplace

Über Zscaler

Zscaler (NASDAQ: ZS) ist ein Pionier und weltweit führender Anbieter von Zero-Trust-Sicherheitslösungen. Die größten Unternehmen der Welt, Betreiber kritischer Infrastrukturen und Regierungsbehörden vertrauen auf Zscaler zum Schutz von Usern, Zweigstellen, Anwendungen, Daten und ™ bekämpft in Kombination mit fortschrittlicher KI täglich Milliarden von Cyberbedrohungen und Richtlinienverstößen und ermöglicht zukunftsfähigen Unternehmen Produktivitätssteigerungen durch Reduzierung von Kosten und Komplexität.

© 2026 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™ sowie weitere unter **zscaler.com/de/legal/trademarks** aufgeführte Marken sind entweder (i) eingetragene Handelsmarken bzw. Dienstleistungsmarken oder (ii) Handelsmarken bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.

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