Leitfaden für CISOs zur Beschleunigung der AWS-Migration mit Zscaler Private Access

Wie Zscaler Private Access (ZPA) die sichere Cloud-Migration und Anwendungsmodernisierung auf AWS unterstützt

E-BOOK



©2026 Zscaler, Inc. Alle Rechte vorbehalten.

Inhaltsverzeichnis



Cloud-Migration und Modernisierung im Jahr 2026 3

Zugriff und Sicherheit als Hemmfaktoren bei der Migration zu AWS 4

Warum Legacy-VPN- und Firewall-Modelle ungeeignet sind 5

Zero Trust: Eine bessere Alternative für die Cloud-Migration zu AWS 6

Was ist Zscaler Private Access (ZPA) 7

Wie ZPA die Migration zu AWS in allen Phasen unterstützt 8

Wie ZPA gängige Migrationsszenarien unterstützt 10

Erwägungen bei der Modernisierung und KI-Einführung 11

Fazit 12

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

Cloud-Migration und Modernisierung im Jahr 2026

Im Jahr 2026 ist die Migration in die Cloud keine Initiative, die irgendwann in der Zukunft ansteht. Sie ist eine geschäftliche Notwendigkeit für jedes Unternehmen. Gartner prognostiziert für dieses Jahr ein Wachstum von 21,3 % bei Public-Cloud-Services, da immer mehr Unternehmen die Migration ihrer Workloads beschleunigen und die Modernisierung in großem Umfang vorantreiben. Trotz dieser Dynamik werden heute noch 42 % der strategischen Workloads in On-Premise-Umgebungen verarbeitet.

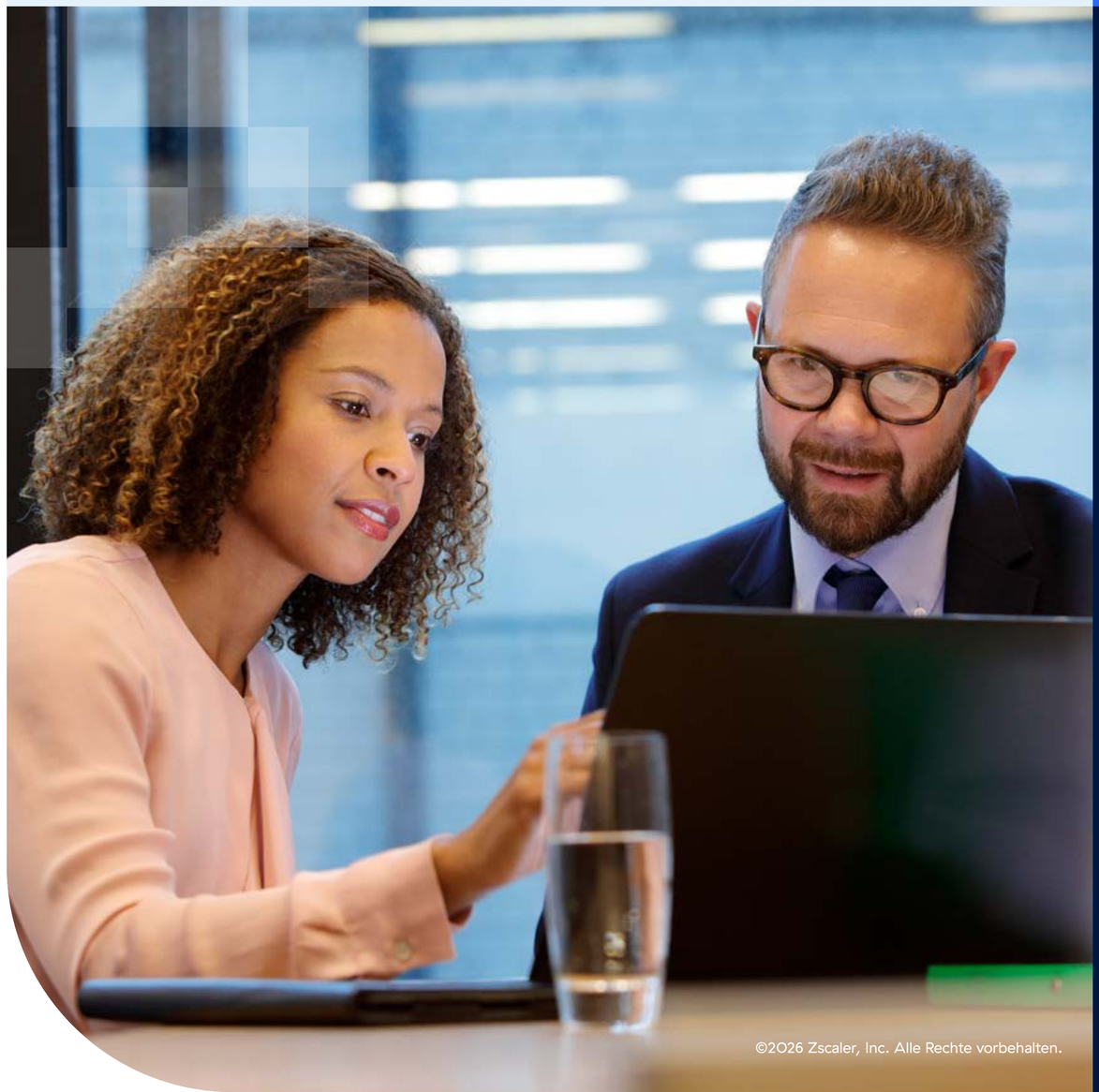
Die Zahlen erzählen eine überzeugende Geschichte darüber, was auf dem Spiel steht. Die Benchmarks des AWS Cloud Adoption Framework zeigen eine Kostenreduzierung von 27 % pro User, eine Verringerung der Ausfallzeiten um 57 % und eine Verringerung der Sicherheitsereignisse um 34 % nach der Migration. Unternehmen, die am AWS Migration Acceleration Program teilnehmen, erreichen ihren ersten Migrationsmeilenstein 41 % schneller als diejenigen, die auf eigene Faust vorgehen. Doch 2026 wurde die Messlatte noch höher gelegt.

Das AWS Migration Acceleration Program umfasst nun neben der herkömmlichen Workload-Migration explizit auch die Transformation mittels generativer und agentenbasierter KI. Der Wechsel zu AWS bedeutet heutzutage nicht mehr nur, Anwendungen zu verlagern und zu migrieren. Sondern es geht darum, die Grundlage für ein KI-fähiges Unternehmen zu schaffen.

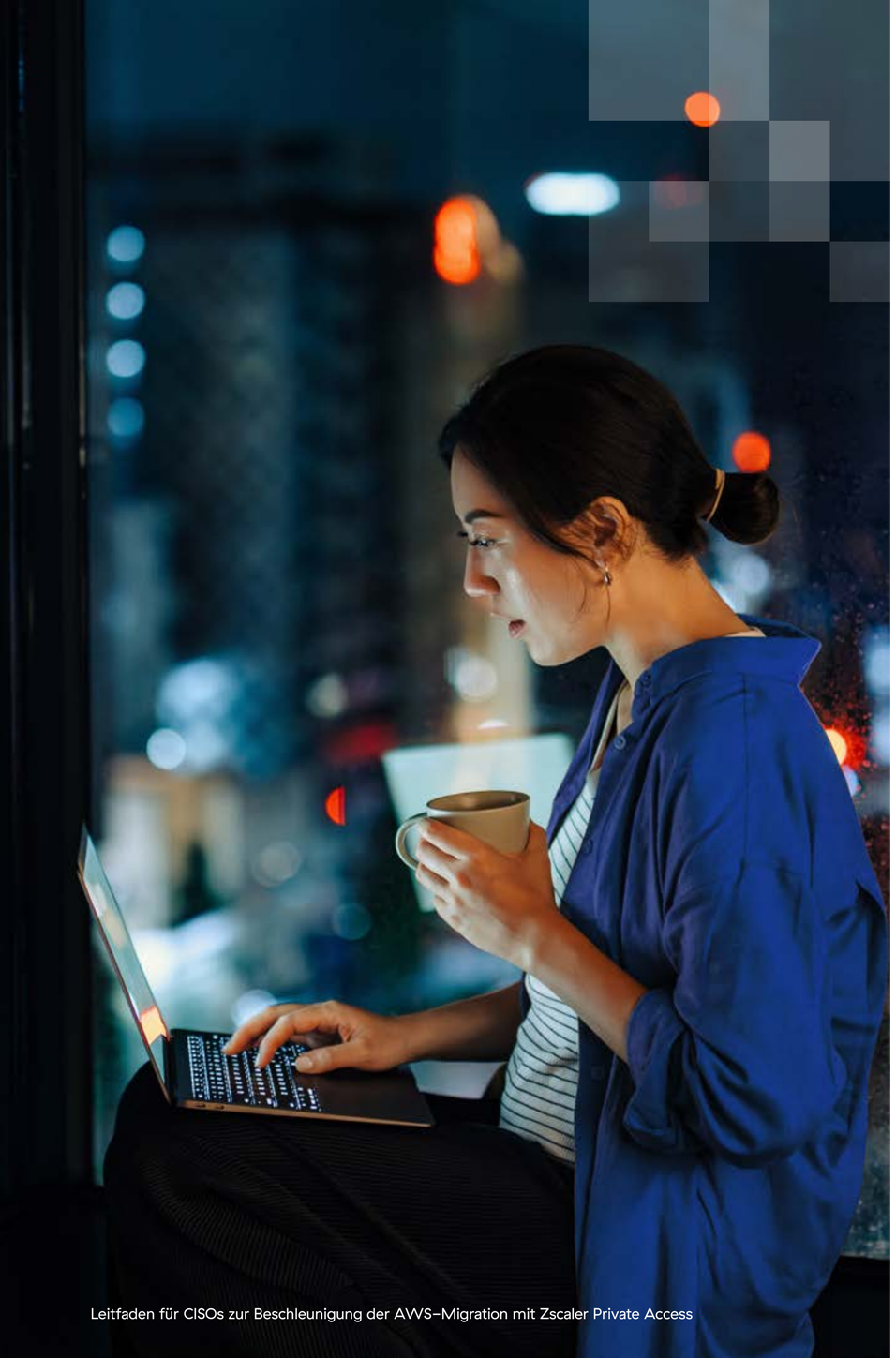
Die Frage lautet nicht mehr, ob Sie migrieren sollen. Die Frage lautet: Ist Ihre Sicherheitsarchitektur so ausgelegt, dass sie mit der Geschwindigkeit mithalten kann, die Ihr Unternehmen im Zeitalter der KI benötigt?

Dennoch verlangsamen sich viele AWS-Migrationen vor oder verzögern sich, wenn der sichere Zugriff sich als Einschränkung erweist. Da Anwendungen zwischen Rechenzentren, Cloud-Umgebungen und hybriden Architekturen verlagert werden, betrachten Unternehmen den Zugriff oft als Herausforderung für die Neugestaltung des Netzwerks. Dieser Ansatz erhöht die Komplexität und verlängert die Zeitpläne.

In diesem E-Book wird erläutert, wie Zscaler Private Access die Herausforderung angeht, indem netzwerkzentrierter Remotezugriff durch identitätsbasierte, anwendungsspezifische Konnektivität ersetzt wird. Dieser Ansatz trägt in allen Phasen des AWS-Migrationsprozesses dazu bei, migrationsbedingte Reibungsverluste zu reduzieren, die Modernisierung zu unterstützen und eine sicherere Grundlage für zukünftige KI-Initiativen zu schaffen.



©2026 Zscaler, Inc. Alle Rechte vorbehalten.



Zugriff und Sicherheit als Hemmfaktoren bei der Migration zu AWS

Cloud-Migrationsprogramme werden oft als Anwendungs- und Infrastrukturprojekte konzipiert. In der Praxis handelt es sich jedoch auch um Projekte zur Transformation von Zugriff und Sicherheit. Selbst wenn eine Workload technisch bereit für die Migration ist, muss das betreffende Unternehmen noch festlegen, wie Mitarbeitende, Auftragnehmer, Geschäftspartner und Administratoren während des gesamten Übergangs sicher darauf zugreifen können. Diese Herausforderung wird häufig unterschätzt. Migrationspläne berücksichtigen zwar Rechenleistung, Speicher, Architektur und Anwendungsabhängigkeiten, verschieben Entscheidungen über Userzugriff und Segmentierung jedoch auf spätere Phasen. In solchen Fällen sind Sicherheits- und Netzwerkfachkräfte gezwungen, Legacy-Kontrollmechanismen unter Zeitdruck an neue Cloud-Bereitstellungsmodelle anzupassen. Das führt häufig zu Nacharbeiten, verzögerten Freigaben und uneinheitlichen Zugriffsrichtlinien in verschiedenen Umgebungen.

Drei Probleme erschweren dies besonders.

- **Erstens** entsteht Komplexität während des Übergangs. Anwendungen werden selten in einem einzigen Schritt von On-Premises zu AWS migriert. Häufiger werden Frontend, Middleware und Datenebenen zu unterschiedlichen Zeitpunkten verschoben. Einige Services verbleiben im Rechenzentrum, während andere zu AWS migriert werden. Während dieser Phase benötigen User weiterhin zuverlässigen Zugriff, und Administratoren müssen Einblick haben, wer auf welche Ressourcen zugreift.

- **Zweitens** sind herkömmliche Zugriffsmodelle eng mit dem Netzwerkstandort verknüpft. Wenn der Zugriff von der VPN-Topologie, Firewall-Regeln, IP-Bereichen oder Annahmen zum internen Routing abhängt, kann jede Anwendungsverschiebung zusätzlichen Entwicklungsaufwand nach sich ziehen. Sicherheitsrichtlinien müssen angepasst, Zugriffspfade erneut validiert und die User Experience kann sich während Umstellungen unerwartet ändern.

- **Drittens** birgt diese Komplexität Geschäftsrisiken. Verzögerungen bei der Gestaltung sicherer Zugriffsrechte können die Migration verlangsamen. Uneinheitliche Richtlinien können die Angriffsfläche vergrößern. Eine schlechte User Experience kann Widerstände gegen Veränderungen hervorrufen und den Supportaufwand erhöhen. In vielen Fällen wird die Gestaltung sicherer Zugriffsrechte zu einer versteckten Abhängigkeit, die Geschwindigkeit, Kosten und Zuverlässigkeit des Migrationsprogramms beeinträchtigt.

Aus diesen Gründen dürfen Zugriff und Sicherheit nicht als Punkte betrachtet werden, die man nachträglich abhaken kann. Vielmehr sollten sie von Anfang an als grundlegende Elemente in die Migrationsstrategie einbezogen werden. Unternehmen, die so vorgehen, sind besser aufgestellt, um Reibungsverluste zu reduzieren, Kontinuität zu gewährleisten und die Sicherheit zu verbessern, wenn Workloads zu AWS verlagert werden.

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

Warum Legacy-VPN- und Firewall-Modelle ungeeignet sind

Herkömmliche VPN- und Firewall-Architekturen wurden entwickelt, um das Vertrauen auf der Grundlage des Netzwerkstandorts zu erweitern. Dieses Modell mag noch funktioniert haben, als die Anwendungen in einem unternehmenseigenen Rechenzentrum konzentriert waren und die meisten User von einer kleinen Anzahl vertrauenswürdiger Standorte aus arbeiteten. Für heutige AWS-Migrationsprogramme ist es ungeeignet.

- **Legacy-Zugriff erhöht das Risiko:** VPNs und ähnliche Remotezugriffstools ermöglichen Usern, auf das gesamte Netzwerk zuzugreifen, anstatt ihren Zugriff auf bestimmte Anwendungen zu beschränken. Sobald der Zugriff gewährt ist, kann der User oder das Gerät möglicherweise auf weite Teile der Umgebung zugreifen. Dies vergrößert die Angriffsfläche und schafft Möglichkeiten für die laterale Ausbreitung von Bedrohungen, falls Zugangsdaten kompromittiert oder Endgeräte infiziert werden. In hybriden Umgebungen tritt das Problem noch deutlicher hervor. Da Anwendungen auf lokale und Cloud-Umgebungen verteilt sind, erschwert der breite Netzwerkzugriff die präzise Kontrolle darüber, welche User auf welche Workloads zugreifen können. Die Sicherheit wird von Segmentierungsebenen abhängig, die oft nicht für ständige Veränderungen ausgelegt sind.

- **Legacy-Architekturen verursachen Kosten und Verzögerungen:** Firewall-Regeln, Zugriffskontrolllisten, VPN-Konzentratoren, Routing-Abhängigkeiten und IP-basierte Richtlinien können Migrationshindernisse darstellen, die Planung, Koordination, Tests und Freigaben erfordern. Während der Migration können sich diese Abhängigkeiten vervielfachen, da die zuständigen Fachkräfte gleichzeitig die Zugriffskontinuität in alten und neuen Umgebungen gewährleisten müssen. Viele Unternehmen betreiben zudem mehrere Sicherheitslösungen, die sich im Laufe der Zeit weiterentwickelt haben. Dies führt zu einer Fragmentierung der Richtlinien und einem erhöhten operativen Aufwand. Anstatt die Migration zu vereinfachen, wird die Sicherheitsarchitektur zu einer weiteren Domäne, die abgestimmt und neu konfiguriert werden muss.

- **Herkömmliche Routing-Methoden beeinträchtigen die User Experience:** Herkömmlicher Remotezugriff basiert häufig auf der Umleitung des Traffics über zentrale Netzwerkstandorte, bevor User mit der Anwendung verbunden werden. Da Anwendungen immer näher an die Cloud-User verlagert werden, kann der Traffic weiterhin über ineffiziente, veraltete Pfade fließen. Dies führt zu höheren Latenzzeiten, inkonsistenter Leistung und zunehmender Frustration der User. Eine schlechte User Experience ist nicht nur lästig, sondern kann auch zu Workarounds, vermehrten Supportanfragen und einem geringeren Vertrauen in die Migration führen.



©2026 Zscaler, Inc. Alle Rechte vorbehalten.



Zero Trust: Eine bessere Alternative für die Cloud-Migration zu AWS

Die Migration zu AWS erfordert ein Zugriffsmodell, das dem User und der Anwendung folgt, statt sich auf ein umfassendes Vertrauen innerhalb des Netzwerks zu verlassen. Unternehmen benötigen eine Möglichkeit, weiterhin sicheren Zugriff zu gewährleisten, wenn Anwendungen verlagert werden, Architekturen sich weiterentwickeln und Umgebungen über längere Zeiträume in hybridem Zustand bleiben. Ein Zero-Trust-Zugriffsmodell ist dafür geradezu prädestiniert.

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

Was ist Zscaler Private Access (ZPA)?

Zscaler Private Access (ZPA) verbindet User ausschließlich mit autorisierten Anwendungen, niemals mit dem Netzwerk. ZPA verifiziert Identität und Kontext, setzt Richtlinien durch und vermittelt sichere Verbindungen über die Zero Trust Exchange (ZTE), anstatt auf standort- oder IP-basiertes Vertrauen zurückzugreifen. Unter Verwendung bestehender Identitätsframeworks wie SAML und MFA stellt ZPA direkte, ausschließlich ausgehende Verbindungen über App-Konnektoren her. Dieser Ansatz eliminiert die Notwendigkeit, eingehende Anwendungen offenzulegen, vereinfacht die Sicherheitsarchitektur und macht private Unternehmensanwendungen für User ohne entsprechende Berechtigungen unzugänglich.

Diese Architektur revolutioniert die Sicherheit, indem sie den Zugriff vom Netzwerk entkoppelt. User werden nicht im Netzwerk platziert und Anwendungen nicht exponiert. Stattdessen wird der Zugriff auf Anwendungsebene auf Basis von Identität und Kontext gewährt. Da dieses Modell den Zugriff von der zugrunde liegenden physischen oder Cloud-Infrastruktur entkoppelt, können Unternehmen Anwendungen zwischen Rechenzentren, VPCs und Clouds migrieren, ohne die User-Konnektivität neu konfigurieren zu müssen. Folglich dient ZPA nicht nur als Lösung für den Remotezugriff, sondern auch als entscheidender Faktor für die AWS-Migration, der gleichzeitig die Angriffsfläche verringert und dem Unternehmen Kontrolle gibt.

1 Anwendungskonnektor

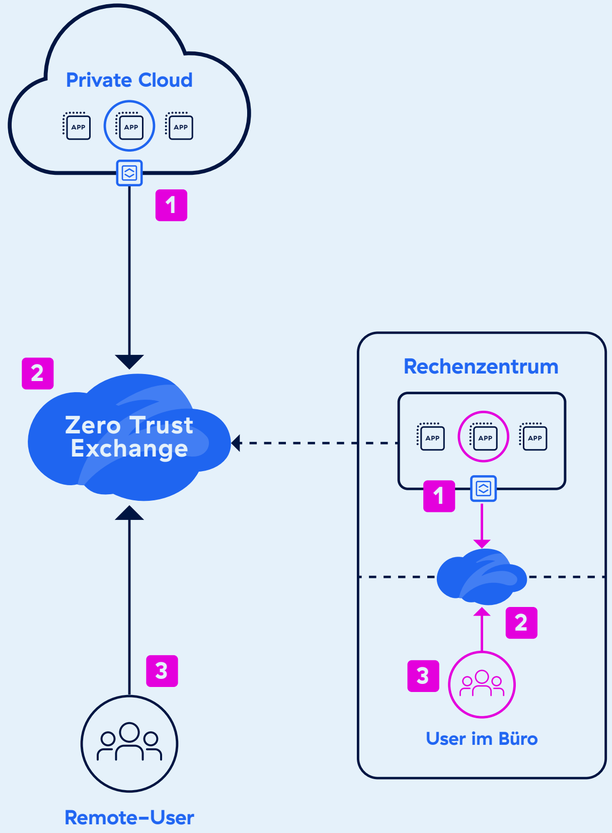
- Bereitgestellt neben Servern und Apps
- Authentifizierte, sichere Schnittstelle zwischen den Anwendungsservern eines Unternehmens und der ZPA-Cloud

2 ZPA Service Edges

- Durchsetzen von Userrichtlinien, sichere Übertragung zu Anwendungskonnektoren
- Öffentliche und private Service Edges stehen zur Unterstützung beider Anwendungsfälle zur Verfügung.

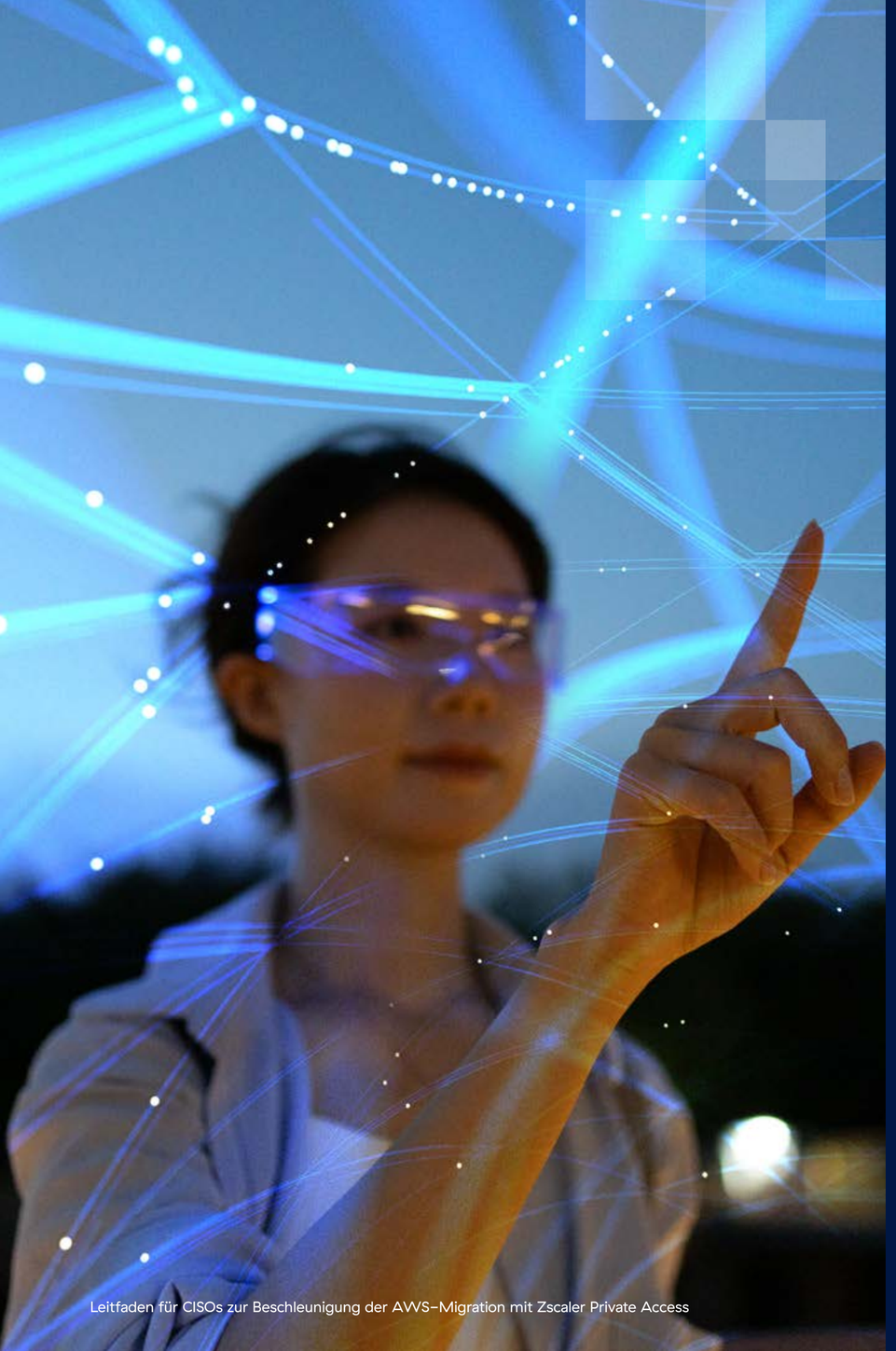
3 Client-Konnektoren

- Ressourcenschonende Anwendung, die auf Ihrem Gerät installiert ist
- Gewährleisten, dass Ihr Traffic und der Zugriff auf interne Anwendungen sicher sind und den Richtlinien Ihres Unternehmens entsprechen



Komponenten von Zscaler Private Access (ZPA)

©2026 Zscaler, Inc. Alle Rechte vorbehalten.



ZPA unterstützt jede Phase der Migration zu AWS

Ein wesentlicher Vorteil von ZPA besteht darin, dass es sämtliche Phasen des AWS Cloud Adoption Framework als Ganzes unterstützt und nicht nur den endgültigen Zugriffszustand nach der Migration der Workloads. Durch die frühzeitige Etablierung eines einheitlichen, anwendungsspezifischen Zugriffsmodells können Unternehmen sicherheitsrelevante Reibungsverluste bei Planung, Übergang, Umstellung und laufendem Betrieb reduzieren.

1. Phase: Vorbereitung und Planung

Herausforderung für Kunden: Die Migrationsbeauftragten vernachlässigen häufig die Sicherheitsplanung, da sie fälschlicherweise annehmen, dass sich bestehende VPNs und Firewalls problemlos auf AWS übertragen lassen. Dies führt zu kostspieligen Neukonzeptionen, wenn die bestehenden Kontrollmechanismen nicht mit dem neuen Cloud-Betriebsmodell kompatibel sind.

Vorteile von ZPA: ZPA ermöglicht identitätsbasierte Zugriffskontrolle von Anfang an. Indem Richtlinien auf Usern, Geräten und Anwendungen anstatt auf Netzwerkstandorten basieren, können die zuständigen Fachkräfte Zugriffsrechte definieren und Multi-Faktor-Authentifizierung (MFA) anwenden, ohne auf endgültige IP-Schemata oder Routing-Entscheidungen warten zu müssen. Dies minimiert Unterbrechungen und den Aufwand für das Änderungsmanagement, da die gewohnten Arbeitsabläufe für die User erhalten bleiben.

Betriebswirtschaftliche und sicherheitsrelevante Ergebnisse: Die Integration von Sicherheit als Grundlage — statt als nachgelagerte Kontrollinstanz — reduziert Architekturänderungen in späten Phasen, beschleunigt die Planung und fördert eine bessere Abstimmung zwischen den Teams, die für Migration und Sicherheit zuständig sind.

2. Phase: Portfolio und Erkennung

Herausforderung für Kunden: Migrationen scheitern oft an der unvollständigen Transparenz der internen Anwendungsnutzung. Dadurch ist es schwierig festzustellen, welche Anwendungen aktiv sind, welche Abhängigkeiten bestehen und welche Prioritäten für die Migration gelten.

Vorteile von ZPA: ZPA gibt verbesserten Einblick in den Zugriff auf private Unternehmensanwendungen und die User-Beziehungen. Dadurch können Unternehmen Workloads anhand der tatsächlichen Nutzung statt anhand von Annahmen priorisieren. Es ermöglicht einen schrittweisen Ansatz, bei dem Anwendungen identifiziert, Richtlinien angepasst und die Segmentierung vor der Migration definiert werden. So werden Risiken und Richtlinienlücken während der Umstellung minimiert.

Betriebswirtschaftliche und sicherheitsrelevante Ergebnisse: Unternehmen profitieren von fundierter Planung, effektiver Priorisierung der Migration und aussagekräftigen Baselines für den Zugriff. Indem Abhängigkeiten frühzeitig im Migrationsprozess aufgedeckt werden, lassen sich böse Überraschungen vermeiden.



3. Phase: Operative Planung und Durchführung

Herausforderung für Kunden: Die Migration von Workloads zu AWS führt zur Entstehung komplexer, heterogener Umgebungen, in denen Anwendungen lokal, in der Cloud oder beides gehostet werden. Die Anpassung der Zugriffsmodelle an diese dynamischen Architekturen führt zu Inkonsistenzen und operativer Komplexität.

Vorteile von ZPA: ZPA stellt für alle Umgebungen, in denen Anwendungen gehostet werden, ein konsistentes identitäts- und anwendungsbasiertes Richtlinienframework bereit. Unternehmen vermeiden so die Neugestaltung des Zugriffs bei jeder Migration und wechseln von einer subnetz- oder IP-basierten Segmentierung zu einem Zugriffsmodell, das sich auf Berechtigungen und Bedingungen konzentriert.

Betriebswirtschaftliche und sicherheitsrelevante Ergebnisse: Vereinfachte operative Planung, höhere Migrationsagilität, reduzierte Abhängigkeiten im Zusammenhang mit Zugriffen und vorhersehbare Anwendererfahrungen während des gesamten Übergangs.

4. Phase: Migration und Validierung

Herausforderung für Kunden: Während der Umstellung lässt sich schwer feststellen, ob die Anwendungsmigrationen erfolgreich und sicher ablaufen, ohne den Userzugriff zu beeinträchtigen.

Vorteile von ZPA: ZPA entkoppelt den Zugriff vom Standort der Workloads und ermöglicht so eine nahtlose Migration zwischen Rechenzentren und AWS, ohne dass User sich an neue Zugriffspfade gewöhnen müssen. Es stellt sicher, dass der Zugriff auf die Anwendung und nicht auf die Netzwerkinfrastruktur fokussiert bleibt und bietet gleichzeitig wichtige Transparenz, um die Sicherheit zu überprüfen und das Verhalten von Richtlinien während der Migration zu überwachen.

Betriebswirtschaftliche und sicherheitsrelevante Ergebnisse: Reduziertes Migrationsrisiko und geringere Beeinträchtigung der User bei verbesserter Governance. Unternehmen profitieren von der Flexibilität, Workloads zu verlagern, ohne komplexe Netzwerkkonfigurationen vornehmen zu müssen.

5. Phase: Laufender Betrieb und zukünftige Investitionen

Herausforderung für Kunden: Nach der Migration benötigen Unternehmen ein skalierbares Betriebsmodell, das hybride Umgebungen unterstützt, ohne die Komplexität bestehender Netzwerke wieder einzuführen.

Vorteile von ZPA: ZPA ermöglicht die globale Verwaltung von richtlinienbasierten Einzelverbindungen zwischen Usern und Anwendungen und beseitigt so den Aufwand komplexer IP-basierter Segmentierung. Es ermöglicht eine präzise Zugriffskontrolle für Mitarbeitende, Auftragnehmer und Drittanbieter in AWS-, On-Premises- und Hybridumgebungen. Dadurch werden zukünftige Modernisierungen unterstützt, ohne auf einen breiten Netzwerkzugriff zurückgreifen zu müssen.

Betriebswirtschaftliche und sicherheitsrelevante Ergebnisse: Unternehmen profitieren von einem flexiblen, nachhaltigen und vereinfachten Betriebsmodell, das fortlaufende Governance und Transformation unterstützt.

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

Wie ZPA gängige Migrationsszenarien löst

Die Migrationsprogramme sind vielfältig und reichen von „Lift and Shift“–Lösungen und partieller Modernisierung bis hin zu Cloud–nativen Neuentwicklungen. ZPA unterstützt diese unterschiedlichen Bereitstellungsmuster mit einem einheitlichen Zugriffsparadigma.

SZENARIO 1

Lift–and–Shift unter Wahrung der Vertraulichkeit der Anwendungen

Viele Anwendungen, insbesondere komplexe Unternehmens–Workloads, werden schrittweise und mit minimalen architektonischen Änderungen in AWS migriert. In solchen Szenarien können Frontend–, Anwendungs– und Datenebenen phasenweise verlagert werden. Einige Komponenten bleiben möglicherweise für eine gewisse Zeit in On–Premise–Umgebungen, während andere in die AWS–Umgebung verlagert werden. ZPA unterstützt dieses Modell, indem es in allen Phasen des Übergangs privaten, anwendungsspezifischen Zugriff gewährleistet.

Die User können sich weiterhin über dieselben identitätsbasierten Kontrollmechanismen mit der Anwendung verbinden, selbst wenn sich der zugrunde liegende Hosting–Standort ändert. Dadurch lässt sich Kontinuität gewährleisten, ohne vertrauliche Anwendungen zu exponieren oder auf einen breiten Netzwerkzugriff zurückzugreifen. Für Unternehmen, die hochwertige oder streng kontrollierte Anwendungen migrieren, kann dies die Lift–and–Shift–Migration besser handhabbar und weniger störend machen.

SZENARIO 2

Selektiver externer Zugriff mit Zero–Trust–Kontrollen

Manche Anwendungen müssen aus geschäftlichen Gründen einem breiteren Userkreis zugänglich gemacht werden, beispielsweise Drittusern, Geschäftspartnern, Auftragnehmern oder anderen externen Teams. Häufig benötigen diese User Zugriff über Geräte, die nicht vom Unternehmen verwaltet werden. In diesen Fällen wollen Unternehmen den Zugriff auf die Anwendung selbst (nicht auf das Netzwerk) erweitern, ohne die Anwendung im Internet zu exponieren oder ihren Datensicherheitsstatus zu schwächen.

ZPA ermöglicht browserbasierten Zero–Trust–Zugriff, indem User nur mit der jeweiligen Anwendung verbunden werden, zu deren Nutzung sie berechtigt sind, ohne dass ein Agent auf ihrem Gerät erforderlich ist. Die User authentifizieren sich über den Identitätsanbieter des Unternehmens, und der Zugriff wird durch identitäts– und kontextbasierte Richtlinien durchgesetzt. Der Zugriff wird über eine vermittelte ausgehende Verbindung zwischen dem Browser des Users und der Anwendung hergestellt, wodurch die Anwendung vor dem öffentlichen Internet verborgen bleibt.

SZENARIO 3

Cloud–native Umgestaltung der Systemarchitektur unter Beibehaltung des privaten Zugriffs

Nicht alle Anwendungen werden in ihrer ursprünglichen Form zu AWS migriert. Viele werden zu Cloud–nativen Services umstrukturiert. Dazu gehören EC2, Container, serverlose Funktionen, verwaltete Datenbanken und verteilte Anwendungskomponenten. Dies erhöht zwar die architektonische Flexibilität, kann aber auch die Verwaltung herkömmlicher netzwerkbasierter Zugriffskontrollen erschweren. ZPA trägt zur Lösung dieses Problems bei, indem der Zugriff auf die Identität und den Anwendungskontext und nicht auf die sich entwickelnde Netzwerktopologie hinter der Anwendung ausgerichtet bleibt.

Vertrauliche Geschäftssysteme, Entwicklungsumgebungen und administrative Schnittstellen können auch dann noch durch detaillierte Richtlinien privat zugänglich bleiben, wenn die Anwendungsarchitektur dynamischer wird. Dies ist insbesondere relevant für regulierte Workloads, Unternehmensplattformen und Modernisierungsprogramme, bei denen sich die Sicherheit parallel zur Architektur weiterentwickeln muss und nicht hinter ihr zurückbleiben darf.

©2026 Zscaler, Inc. Alle Rechte vorbehalten.



Bedeutung in der Praxis

Die Migration von Workloads zu AWS findet zunehmend im Rahmen eines umfassenden Modernisierungsprogramms statt. Dabei verlagern Unternehmen nicht einfach nur ihre Infrastruktur. Sie aktualisieren Anwendungsarchitekturen, optimieren Betriebsmodelle, führen Cloud-native Services ein und expandieren in neue Bereiche wie Datenplattformen, Automatisierung und KI. Dies unterstreicht die Bedeutung der bewussten Gestaltung von Zugriffspfaden, anstatt sie zu verringern.

Modernisierte Umgebungen sind oft stärker verteilt als die Systeme, die sie ersetzen. Sie können unterschiedliche Servives, Entwicklungspipelines, hybride Abhängigkeiten und eine breitere Usergruppe umfassen. In solchen Umgebungen wird es noch schwieriger, ein breites, netzwerkzentriertes Vertrauen zu rechtfertigen und aufrechtzuerhalten. Der Zugriff muss granularer abgestuft, kontextbezogener und in dynamischen Architekturen leichter zu kontrollieren sein.

Das Gleiche gilt für KI-Initiativen. Unternehmen, die KI-bezogene Anwendungen, Entwicklungsumgebungen und vertrauliche Daten-Workflows auf AWS verlagern, benötigen eine strengere Kontrolle darüber, wer auf diese Ressourcen von welchen Geräten und unter welchen Bedingungen zugreifen kann.
Diese Umgebungen umfassen oft abteilungsübergreifende Teams, Drittuser und hochgradig dynamische Arbeitsabläufe. Zero Trust ist daher nicht einfach nur eine Verbesserung der Sicherheit; es ist eine Governance-Anforderung, die ein identisches anwendungsspezifisches Zugriffsmodell für Migrations-, Modernisierungs- und KI-nahe Umgebungen anwendet.

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

Fazit

Die Migration zu AWS verlangsamt sich oft, weil der sichere Zugriff zu einer versteckten Komplexitätsursache wird. Solange User, Anwendungen und Richtlinien an Legacy-VPN- und Firewall-Modelle gebunden sind, lassen sich alle Schritte der Migration schwieriger planen, validieren und skalieren.

Zscaler stellt eine Alternative bereit. Durch Ersetzen des netzwerkzentrierten Zugriffs durch identitätsbasierte, anwendungsspezifische Konnektivität unterstützt Zscaler Private Access (ZPA) Unternehmen dabei, die Angriffsfläche zu verringern, Richtlinien zu vereinfachen und einheitliche Anwendererfahrungen in sämtlichen Phasen der Migrationsleben zu gewährleisten. Es unterstützt Planung, Ermittlung, Bereitstellung, Validierung und laufenden Betrieb mit einem Modell, das besser auf AWS-Umgebungen abgestimmt ist.

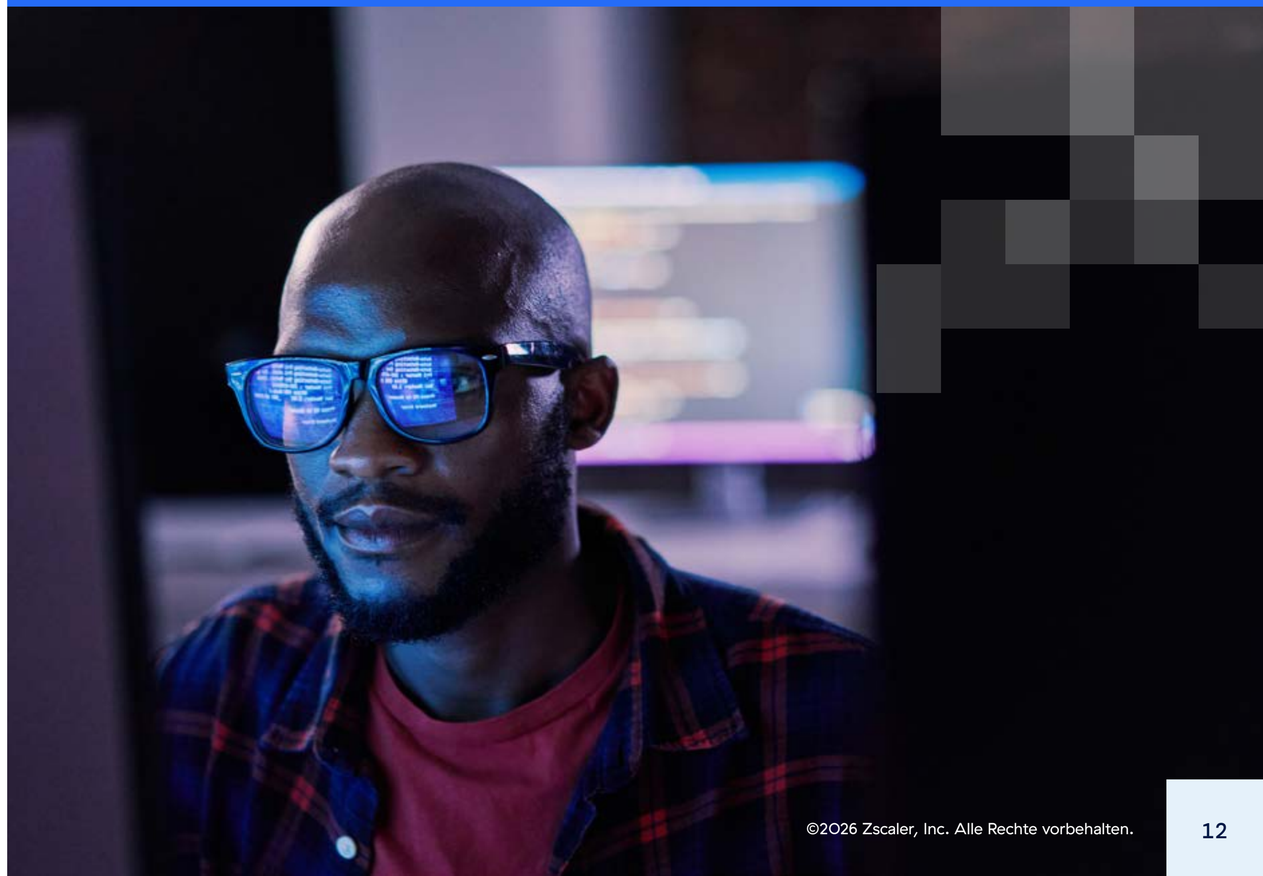
Dies ist nicht nur für die eigentliche Migration von Bedeutung. Da Unternehmen ihre Modernisierung, Cloud-native Transformation und KI-gestützte Initiativen weiter vorantreiben, steigt die Nachfrage nach präzisem Zugriff nach dem Prinzip der minimalen Rechtevergabe stetig an. Ein Zero-Trust-Zugriffsmodell verbessert daher nicht nur die Sicherheit. Es ist eine grundlegende Voraussetzung für die Agilität im Cloud-Betrieb. Unternehmen, die auf AWS migrieren und modernisieren, müssen sicheren Zugriff von Anfang an mitberücksichtigen. Er darf der Architektur nicht nachträglich aufgepfropft, sondern muss in ihr Fundament eingebaut werden. Zscaler trägt dazu bei, dies zu ermöglichen.

Quellen:
Einfache und sichere Migration zu AWS mit Zscaler
Framework für die AWS-Cloud-Bereitstellung
Gartner®
Zscaler für AWS (Partnerseite)

ZPA ist auf dem AWS Marketplace verfügbar.

ZPA ist auf dem AWS Marketplace verfügbar und erleichtert Unternehmen die Beschaffung, Bereitstellung und Verwaltung des sicheren Anwendungszugriffs in ihren bestehenden AWS-Umgebungen. Ausführliche Lösungsdetails, Demoanfragen und Kaufoptionen finden Sie auf der Produktseite von **ZPA-im Marketplace**.

Um mehr über Zscaler auf dem AWS Marketplace zu erfahren, besuchen **Sie unser Verkäuferprofil**.



©2026 Zscaler, Inc. Alle Rechte vorbehalten.

Schneller agieren.
Dauerhaft schützen.

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