A CISO's Guide to Accelerating AWS Migration with Zscaler Private Access

How Zscaler Private Access (ZPA) Supports Secure Cloud Migration and App Modernization on AWS

EBOOK

Table of Contents

Cloud Migration and Modernization in 2026

In 2026, cloud migration is no longer a future initiative. It is the business imperative of every enterprise. Gartner forecasts 21.3% growth in public cloud services this year, driven by organizations accelerating workload migration and embracing modernization at scale. Yet despite this momentum, 42% of strategic workloads remain on-premises today.

The numbers tell a compelling story about what is at stake. AWS Cloud Adoption Framework benchmarks show a 27% reduction in cost per user, a 57% decrease in downtime, and a 34% decrease in security events post-migration. Organizations participating in the AWS Migration Acceleration Program are reaching their first migration milestone 41% faster than those going it alone. But 2026 has raised the bar further.

The AWS Migration Acceleration Program now explicitly encompasses generative and agentic AI transformation alongside traditional workload migration. Moving to AWS is no longer just about lifting and shifting applications. It is about building the foundation for an AI-ready enterprise.

The question is no longer whether to migrate. It is whether your security architecture is built to move at the speed your business requires in the age of AI.

Yet many AWS migrations still slow down or get delayed when secure access becomes a constraint. As applications move across datacenters, cloud environments, and hybrid architectures, organizations often treat access as a network redesign challenge. That approach adds complexity and extends timelines.

This e-book explores how Zscaler Private Access addresses the challenge by replacing network-centric remote access with identity-based, application-specific connectivity and how that approach helps reduce migration friction, support modernization, and build a more secure foundation for future AI initiatives throughout the AWS migration journey.

Access and Security Delay AWS Migration

Cloud migration programs are often framed as application and infrastructure projects. In practice, however, they are also access and security transformation projects. Even when a workload is technically ready to move, organizations still need to determine how employees, contractors, partners, and administrators will reach it securely throughout the transition. This challenge is frequently underestimated. Migration plans may account for compute, storage, architecture, and application dependencies, but defer user access and segmentation decisions until later stages. When that happens, security and networking teams are forced to adapt legacy controls to new cloud delivery models under time pressure. The result is often rework, delayed approvals, and inconsistent access policies across environments.

Three issues make this particularly difficult.

- **First,** migration creates transitional complexity. Applications rarely move from on-premises to AWS in a single step. More often, front-end, middleware, and data tiers move at different times. Some services remain in the datacenter while others shift to AWS. During this period, users still need reliable access, and administrators need visibility into who is accessing what.

- **Second,** traditional access models are tightly coupled to network location. If access depends on VPN topology, firewall rules, IP ranges, or internal routing assumptions, every application move can trigger additional design work. Security policies must be adjusted, access paths must be revalidated, and user experience may change unexpectedly during cutovers.

- **Third,** this complexity creates business risk. Delays in secure access design can slow migration milestones. Inconsistent policies can increase exposure. Poor user experience can generate resistance to change and increase support burden. In many cases, access design becomes a hidden dependency that affects the speed, cost, and confidence of the migration program.

For these reasons, access and security should not be treated as a downstream box to check. They should be factored in as foundational elements of the migration strategy upfront. Organizations that do so are better positioned to reduce friction, maintain continuity, and improve security as workloads move to AWS.

Why Legacy VPN and Firewall Models are the Wrong Fit

Traditional VPN and firewall architectures were designed to extend trust based on network location. That model may have been workable when applications were concentrated inside a corporate datacenter and most users operated from a small number of trusted locations. It is a poor fit for modern AWS migration programs.

- **Legacy Access Expands Risk:** VPNs and similar remote access tools place users onto the network rather than limiting them to specific applications. Once access is granted, the user or device may be able to reach broad segments of the environment. This increases the attack surface and creates opportunities for lateral movement if credentials are compromised or endpoints are infected. In hybrid environments, the problem becomes more pronounced. As applications are distributed across on-premises and cloud environments, broad network access makes it harder to maintain precise control over which users can reach which workloads. Security becomes dependent on segmentation layers that were often not designed for constant change.

- **Legacy Architectures Add Cost and Delay:** Firewall rules, access control lists, VPN concentrators, routing dependencies, and IP-based policies can all become migration friction points requiring planning, coordination, testing, and governance approvals. During migration, these dependencies can multiply because teams must maintain access continuity across old and new environments at the same time. Many organizations also operate multiple security point products that evolved over time. This creates policy fragmentation and operational overhead. Rather than simplifying migration, the security stack becomes another domain that must be reconciled and rejigged.

- **Legacy Routing Degrades the User Experience:** Traditional remote access often depends on backhauling or hairpinning traffic through central network locations before users reach the application. As applications move closer to cloud users, traffic may still flow through inefficient legacy paths. The result is higher latency, inconsistent performance, and more user frustration. Poor user experience is not just an inconvenience. It can drive workarounds, increase support requests, and undermine confidence in the migration effort.

Zero Trust: A Better Fit for AWS Cloud Migration

AWS migration requires an access model that follows the user and the application without depending on broad network trust. Organizations need a way to maintain secure access as applications move, architectures evolve, and environments remain hybrid for extended periods. That is the role a zero trust access model is designed to play.

What is Zscaler Private Access (ZPA)?

Zscaler Private Access (ZPA) connects users only to authorized applications, never the network. ZPA verifies identity and context, enforces policy, and brokers secure connections via the Zero Trust Exchange (ZTE) rather than relying on location or IP–based trust. Utilizing existing identity frameworks like SAML and MFA, ZPA establishes direct, outbound–only connections via App Connectors. This approach eliminates the need for inbound application exposure, simplifying security architecture while hiding private applications from unauthorized users.

This architecture transforms security by decoupling access from the network. Users are not placed on the network, and applications are not exposed. Instead, access is granted at the application level based on identity and context. Because this model abstracts access from underlying physical or cloud infrastructure, organizations can migrate applications between datacenters, VPCs, and clouds without reconfiguring user connectivity. Consequently, ZPA serves not only as a remote access solution but as a critical enabler for AWS migration, simultaneously reducing the attack surface and maintaining control.

1 App Connector

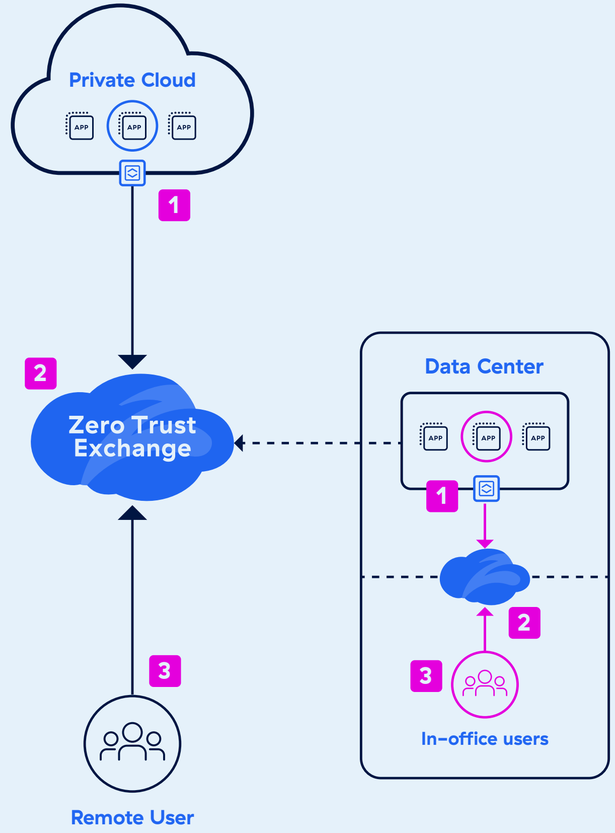
- Deployed ajacent to serves and apps
- Provide authenticated secure interface between an org's application servers and the ZPA cloud

2 ZPA Service Edges

- Enforce user policies and provide secuire transport to App Connectors
- Public and Private Service Edges are available to support either use case

3 Client Connectors

- A lightweight application installed on your device
- Ensure your internet traffic and access to internal apps are secure and in complance with your org's policies



Zscaler Private Access (ZPA) Components

ZPA Supports Each Phase of Migration to AWS

A key advantage of ZPA is that it supports the AWS Cloud Adoption Framework phases as a whole, not just the final access state after workloads have moved. By establishing a consistent, application-specific access model early, organizations can reduce security-related friction across planning, transition, cutover, and ongoing operations.

Phase 1: Preparation and Planning

Customer Challenge: Teams often defer security design, incorrectly assuming legacy VPNs and firewalls easily extend to AWS. This leads to costly redesigns when legacy controls fail to align with the new cloud operating model.

How ZPA Helps: ZPA enables identity-based access from the start. By basing policies on users, devices, and applications rather than network location, teams can define access and apply MFA without waiting for final IP schemes or routing decisions. This minimizes disruption and change management overhead by keeping familiar workflows for users.

Business and Security Outcome: Integrating security as a foundation—rather than a downstream gate—reduces late-stage architecture changes, accelerates planning, and fosters better alignment between migration and security teams.

Phase 2: Portfolio and Discovery

Customer Challenge: Migrations often falter due to incomplete visibility into internal application usage, making it difficult to determine which apps are active, their dependencies, and prioritization for migration.

How ZPA Helps: ZPA enhances visibility into private application access and user relationships, allowing organizations to prioritize workloads based on actual usage rather than assumptions. It enables a phased approach, where applications are identified, policies are tuned, and segmentation is defined before migration, minimizing exposure and policy gaps during cutover.

Business and Security Outcome: Organizations achieve more informed planning, effective migration prioritization, and stronger access baselines, reducing surprises by surfacing dependencies early in the migration process.

Phase 3: Operational Planning and Delivery

Customer Challenge: Migrating workloads to AWS creates complex, mixed environments where applications reside on-premises, in the cloud, or both. Adapting access models to these changing architectures causes inconsistency and operational complexity.

How ZPA Helps: ZPA provides a consistent, identity- and application-based policy framework regardless of application location. Teams avoid redesigning access for every migration pattern, moving away from subnet or IP-based segmentation to a model focused on user access rights and conditions.

Business and Security Outcome: Simplified operational planning, better migration agility, reduced access-related dependencies, and a predictable user experience throughout the transition.

Phase 4: Migration and Validation

Customer Challenge: During cutover, teams struggle to verify that application migrations are successful and secure without disrupting user access.

How ZPA Helps: ZPA decouples access from workload location, allowing seamless migration between datacenters and AWS without requiring users to change how they connect. It ensures access remains centered on the application rather than network infrastructure, while providing critical visibility to validate security and monitor policy behavior during transition.

Business and Security Outcome: Reduced migration risk and user disruption while improving governance. Organizations gain the flexibility to move workloads without needing complex network reconfiguration.

Phase 5: Ongoing Operations and Future Investment

Customer Challenge: Post-migration, organizations need a scalable operating model that supports hybrid environments without reintroducing legacy network complexity.

How ZPA Helps: ZPA facilitates per-user, per-application policy management globally, eliminating the burden of complex IP-based segmentation. It enables precise access control for employees, contractors, and third parties across AWS, on-premises, and hybrid setups, ensuring future modernization without reverting to broad network access.

Business & Security Outcome: Organizations achieve a flexible, sustainable, and simplified operating model that supports ongoing governance and transformation.

How ZPA Addresses Common Migration Scenarios

Migration programs vary, from “lift-and-shift” and partial modernization to cloud-native redesigns. ZPA supports these diverse delivery patterns with a unified access paradigm.

SCENARIO 1

Lift-and-Shift While Keeping Applications Private

Many applications, especially complex enterprise workloads, are migrated incrementally into AWS with minimal architectural change. In these scenarios, front-end, application, and data tiers may move in phases. Some components may remain on-premises for a period of time while others shift into AWS. ZPA supports this model by preserving private, application-specific access throughout the transition.

Users continue to connect to the application through the same identity-based controls, even as the underlying hosting location changes. This reduces the need to expose sensitive applications or rely on broad network access to preserve continuity. For organizations moving high-value or tightly controlled applications, this can make lift-and-shift migration more manageable and less disruptive.

SCENARIO 2

Selective External Access with Zero Trust Controls

Some applications need to be made accessible to a broader set of users for business reasons for third-party users, partners, contractors, or other external teams. Often, these users need access from devices not managed by the organization. In these cases, organizations want to extend access to the application itself, and not the network, without exposing the app to the internet or weakening its data security posture.

ZPA enables browser-based Zero Trust access by connecting users only to the specific application they are authorized to use, without requiring an agent on their device. Users authenticate through the organization’s identity provider, and access is enforced through identity- and context-based policy. Access is established through a brokered inside-out connection between the user’s browser and the application, which helps keep the application hidden from the public internet.

SCENARIO 3

Cloud-Native Re-Architecture with Private Access Preserved

Not all applications move to AWS in their original form. Many are re-architected into cloud-native services that may span EC2, containers, serverless functions, managed databases, and distributed application components. This increases architectural flexibility, but it can also make traditional network-based access control harder to manage. ZPA helps by keeping access centered on identity and application context rather than on the evolving network topology behind the application.

Sensitive business systems, development environments, and administrative interfaces can remain privately accessible under granular policy even as the application architecture becomes more dynamic. This is especially relevant for regulated workloads, enterprise platforms, and modernization programs in which security must evolve alongside architecture, not lag behind it.

Why This Matters

Migration of workloads to AWS is increasingly a part of an enterprise's broader modernization agenda. Organizations are not simply relocating infrastructure; they are updating application architectures, streamlining operating models, adopting cloud-native services, and expanding into new areas such as data platforms, automation, and AI. This raises the importance of access design rather than reducing it.

Modernized environments are often more distributed than the systems they replace. They may involve multiple services, development pipelines, hybrid dependencies, and a broader mix of users. In these environments, broad network-centric trust becomes even harder to justify and maintain. Access must become more granular, more context-aware, and easier to govern across changing architectures.

The same is true for AI initiatives. As organizations bring AI-related applications, development environments, and sensitive data workflows onto AWS, they need tighter control over who can access those resources, from which devices, and under what conditions. These environments often involve cross-functional teams, third parties, and rapidly evolving workflows. Zero trust is therefore not simply a security enhancement; it is a governance requirement, applying the same application-specific access model across migration, modernization, and AI-adjacent environments.

Bottom Line

AWS migration often slows because secure access becomes a hidden source of complexity. When users, applications, and policies are still tied to legacy VPN and firewall models, every migration step becomes harder to plan, validate, and scale.

Zscaler offers a different approach. By replacing network-centric access with identity-based, application-specific connectivity, Zscaler Private Access (ZPA) helps organizations reduce attack surface, simplify policy, and maintain a more consistent user experience across the migration lifecycle. It supports planning, discovery, delivery, validation, and ongoing operations with a model that is better aligned to AWS environments.

This matters beyond migration alone. As organizations continue into modernization, cloud-native transformation, and AI-driven initiatives, the need for precise, least-privilege access only increases. A zero trust access model is therefore not only a security improvement. It is a foundational enabler of cloud operating agility. For organizations migrating and modernizing on AWS, secure access should not be an afterthought. It should be part of the architecture from the beginning. Zscaler helps make that possible.

Sources:
Migrate to AWS Simply and Securely with Zscaler
AWS Cloud Adoption Framework
Gartner®
Zscaler for AWS partner page

ZPA is Available on the AWS Marketplace

ZPA is available on AWS Marketplace, making it easier for organizations to procure, deploy, and manage secure application access within their existing AWS environments. For in-depth solution details, request a demo or view purchase options, go to the **ZPA marketplace listing**.

To learn more about Zscaler on the AWS Marketplace, visit our **seller profile**.

Act Fast. Stay Secure.

About Zscaler

Zscaler (NASDAQ: ZS) is a pioneer and global leader in zero trust security. The world's largest businesses, critical infrastructure organizations, and government agencies rely on Zscaler to secure users, branches, applications, data & devices, and to accelerate digital transformation initiatives. Distributed across more than 160 data centers globally, the Zscaler Zero Trust Exchange™ platform combined with advanced AI combats billions of cyber threats and policy violations every day and unlocks productivity gains for modern enterprises by reducing costs and complexity.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**