



The cloud challenge: Expand quickly but safely

Extend Zero Trust Protection Across Your AWS Cloud Investment

EBOOK



Available in
AWS Marketplace

©2026 Zscaler, Inc. All rights reserved.

Table of Contents

The cloud challenge: Expand quickly but safely	3
Zscaler’s modern, comprehensive, cloud-first solution	4
ZPA: A seamless, cloud-first, zero-trust access solution for private apps	5
Zero Trust Cloud: A superior cloud workload security solution	6
ZDX: Fast, seamless experiences for end users	7
A joint solution that’s easily deployed and quickly operational	8
Ready to transform your cloud security?	9

The cloud challenge: Expand quickly but safely

Legacy network-based access controls such as VPNs are not ideal modern cloud environments. So what are the options?

More than 94–96%¹ of global enterprises have adopted cloud services, with AWS market share now accounting for 30%² of the global cloud infrastructure market. The benefits of cloud adoption are undeniable, from cost savings to agile scalability. Businesses that operate in the cloud face two new challenges: managing access and operations amidst the growing shift to remote and hybrid work structures, and the increasingly sophisticated threat posed by malware and ransomware.

Historically, implementing a secure environment required a network-centric Virtual Private Network (VPN), which sacrificed speed, ease of use, and flexibility in favor of control. Today, as businesses migrate to the cloud and the scale of IT operations grows, the disadvantages of using a VPN become more significant.

At its foundation, a VPN is not designed to provide inherently secure internet access. This puts the burden on the remote workers to have a strong internet connection and up-to-date security measures. As companies that are moving to the cloud employ users who are working from anywhere, inbound connections have expanded, widening the opportunity for DDoS attacks. This, in turn, adds to the complexity of access segmentation amidst reduced visibility into who is doing what on the network. Ultimately, these hurdles limit scalability, increase costs, hinder productivity, and detract from the user experience for employees. In some cases, it also impacts the ultimate end user — the customer.

These quandaries are why Zscaler, a leading zero trust exchange disrupting the network and security industry, works so well with AWS. As an AWS Advanced Technology Partner, Zscaler provides security-as-a-service based on a zero trust model to help businesses achieve true cloud transformation — securely and simply — now and in the future.





Zscaler by the numbers

EACH DAY, ZSCALER:

Blocks

9B+

threats

Processes

750B+

transactions

Provides

250K+

unique security updates

Zscaler's modern, comprehensive, cloud-first solution

A configurable product suite to simplify access and strengthen security, built for hybrid-cloud complexity

Whether a business is looking to shift workloads to the cloud or simply move away from VPN, the verdict is in: Pairing Zscaler and AWS offers top tier security and great user experience through cutting-edge technology and a zero trust model.

Zscaler's application-centric security services are built in the cloud from the ground up, replacing the traditional inbound/outbound gateways for a more modern approach (ideal for companies running on AWS). Three core services help AWS customers make the most of their cloud operations:

Zscaler Private Access (ZPA) makes VPN obsolete by connecting users to applications — not networks — removing applications from the internet for a more secure environment and reduced backend complexity (smoother management of the behind-the-scenes tools and operations with which users don't interact).

Zscaler Zero Trust Cloud (ZTC) centralizes and standardizes workload security management across all clouds through a single, consistent framework, enabling identity-based segmentation, consistent policy enforcement, and unified visibility across hybrid and multicloud environments.

Zscaler Digital Experience Monitoring (ZDX) is a multi-tenant cloudbased monitoring platform that probes,

benchmarks, and measures digital experiences for every single user within an organization.

Together, Zscaler and AWS help organizations bring the future to their front door with:

- Always-on access that improves end user experiences
- More efficient routing that reduces latency and translates to faster time to production
- Stronger, more comprehensive security posture to eliminate threats
- Faster app migration to accomplish minimal downtime
- Increased business agility for a competitive edge
- Lowered costs to free up funds that are better spent elsewhere in the business

While these tools help any business become future-proof, they demonstrate particular value in high-stakes use cases. For example, Zscaler removes many of the technical headaches that IT teams face during mergers and acquisitions. Providing a far less complex integration process while also enforcing best practices in security, Zscaler has helped businesses reduce their technical setup process from months to weeks. Merged companies can connect employees directly to applications without the pain or delay of creating or moving networks.

ZPA: A seamless, cloud-first, zero trust access solution for private apps

Replace clunky VPNs with frictionless access that keeps private apps off the Internet—and invisible to outside threat actors

Once the best option for private access, VPNs have proven less effective in a cloud-based world, essentially routing a user into a network only to send them back out. Traversing the globe to pass through various touchpoints, from firewall to load balancers, app connections for remote workers bring in even more steps. Additionally, VPN requires users to understand which profile they need to use and which resources will allow them access to connect to the network—not an ideal user experience, particularly for less techsavvy employees.

Keep your satellite offices in orbit

ZPA provides secure remote access to apps without a VPN—totally off the network, and never reliant on IP-centric physical or virtual appliances. It manages authorized user access before, during, and after app migration to AWS using a much more efficient and secure pathway—a zero trust, software-defined perimeter (SDP) solution that leverages an inside-out connection established from an AWS App Connector in Zscaler's global security cloud. (It's also complementary to AWS Security Groups, as well as AWS Direct Connect.) Regardless of where a user is trying to connect to internal applications, ZPA translates to swifter app migration, lowered costs, and a reduced threat target even for businesses still relying on a private datacenter.

ZPA Northstar: How GROWMARK Keeps Food Production Going

GROWMARK, a North American agricultural company that provides various materials and services to sustain crop growth, hosts employees out of more than 500 rural locations — so the company is familiar with the challenges of unreliable internet. Once the COVID-19 pandemic arrived and the supply chain took a hit, it was more important than ever that operations went smoothly. In its efforts to modernize, GROWMARK moved hundreds of apps to AWS but also hosted some on premises, and needed a solution that could work with its hybrid structure. After selecting ZPA, GROWMARK was able to provide employees with a more reliable connection while also removing public interfaces from their private environment, ultimately reducing its attack surface. At the height of the pandemic, 98% of GROWMARK's staff was connecting to ZPA with virtually no issues.





Zero Trust Cloud: A superior cloud workload security solution

Transform your workload security from firewalls to Zero Trust

Businesses operating across hybrid and multicloud environments are discovering that legacy network-centric security models are not effective for securing modern workloads. As applications and services move across data centers, private clouds, and public cloud environments, the traditional controls that once helped segment and secure traffic become harder to manage and scale. Static IP-based rules, inconsistent policy models, and disconnected security tools create complexity, reduce visibility, and increase the risk of lateral movement. Added to the mix is the burden of securing east-west, ingress, and egress traffic consistently, making it harder for IT and security teams to keep up.

In the cloud, there's zero room for error

Zscaler Zero Trust Cloud applies zero trust principles so that AWS workloads are never implicitly trusted based on network location. This already puts businesses ahead of the curve, as organizations increasingly look to modernize security for distributed applications and infrastructure. With ZTC, businesses can centralize and standardize workload security management across hybrid and multicloud environments, providing unified visibility and consistent policy enforcement for workloads everywhere they run.

ZTC Northstar: How FICO secures production workloads in the cloud

Analytics software company FICO is advancing its cloud transformation while continuing to support applications that still reside in data centers. As more of its production workloads move to AWS, the company needed a consistent way to extend security controls across cloud environments without relying on fragmented approaches. To support this shift, FICO adopted Zscaler Cloud Connectors to securely connect AWS accounts to Zscaler services, extending the same protections used for users and private application access to cloud workloads. With workloads segmented by zone and AWS account today, FICO is now moving toward more granular segmentation as it expands its cloud footprint and strengthens control over workload security management.

ZDX: Fast, seamless experiences for end users

Gain deep, actionable insights into your UX based on a unified view of app, endpoint, and CloudPath performance metrics

As consumers, we have become accustomed to a gold standard of user experience—to the point where a temporary social media outage makes headlines. While businesses were starting to master the user experience with in-office technology, bottlenecks have become more common as remote and hybrid teams wrestle with hurdles like poor internet connections and a variety of (sometimes outdated) personal mobile devices. When this happens in the form of time-outs and constant reconnections, help tickets pile up and work goes undone — putting IT in a pressure cooker to figure out the cause (and resolution) of unique issues.

Bring frustration-free flights to every end user

ZDX is a multi-tenant cloud-based monitoring platform that probes, benchmarks, and measures the digital experiences for every single user within your organization, no matter where they are. In real time, ZDX will triage what's causing a problem (for example, the internet connection vs. the ISP provider) and then deploys its remote trouble shooting capabilities. Analytics measures performance over time by location, user, and department to identify trends and inform improvements. The result? True Secure Access Server Edge (SASE) architecture that materializes as a superior user experience (and far fewer IT tickets).

ZDX Northstar: How Liberty Mutual improved the employee experience

Liberty Mutual Insurance could guarantee their data centers and ISP bandwidth, but couldn't guarantee what the internet looked like for employees working from home — something that everyone experienced en masse in 2020. Starting with 100 users to deliver proof of concept, Liberty's security team started rolling out ZDX to users with long-term issues as an initial use case, which made it possible to hand off issues to the Level 2 Helpdesk team which could easily resolve user issues with home networks. They've now integrated ZDX across the organization, pinpointing and eliminating service provider latency issues, wireless router problems, memory leaks on desktop computers, and ISP issues around page fetch time, among others.

A joint solution that's easily deployed and quickly operational

With a deployment process built for speed and Zscaler Client Connector managing access, your teams can be up and running in minutes

Moving to a new platform and IT infrastructure can be complex and prolonged. To address this, Zscaler built the adoption process around speed and simplicity—making secure cloud-based operations and smooth transitions easy with Zscaler and AWS.

While **ZPA**, **ZIA**, and **ZDX** can each stand alone, they are best when used together to build out application access based on a well-architected framework. At the heart of their processes is the Zscaler Client Connector (ZCC).

ZPA uses the Client Connector to connect users to private applications using a Zero Trust approach, but Browser Access is also available for web-only private applications.

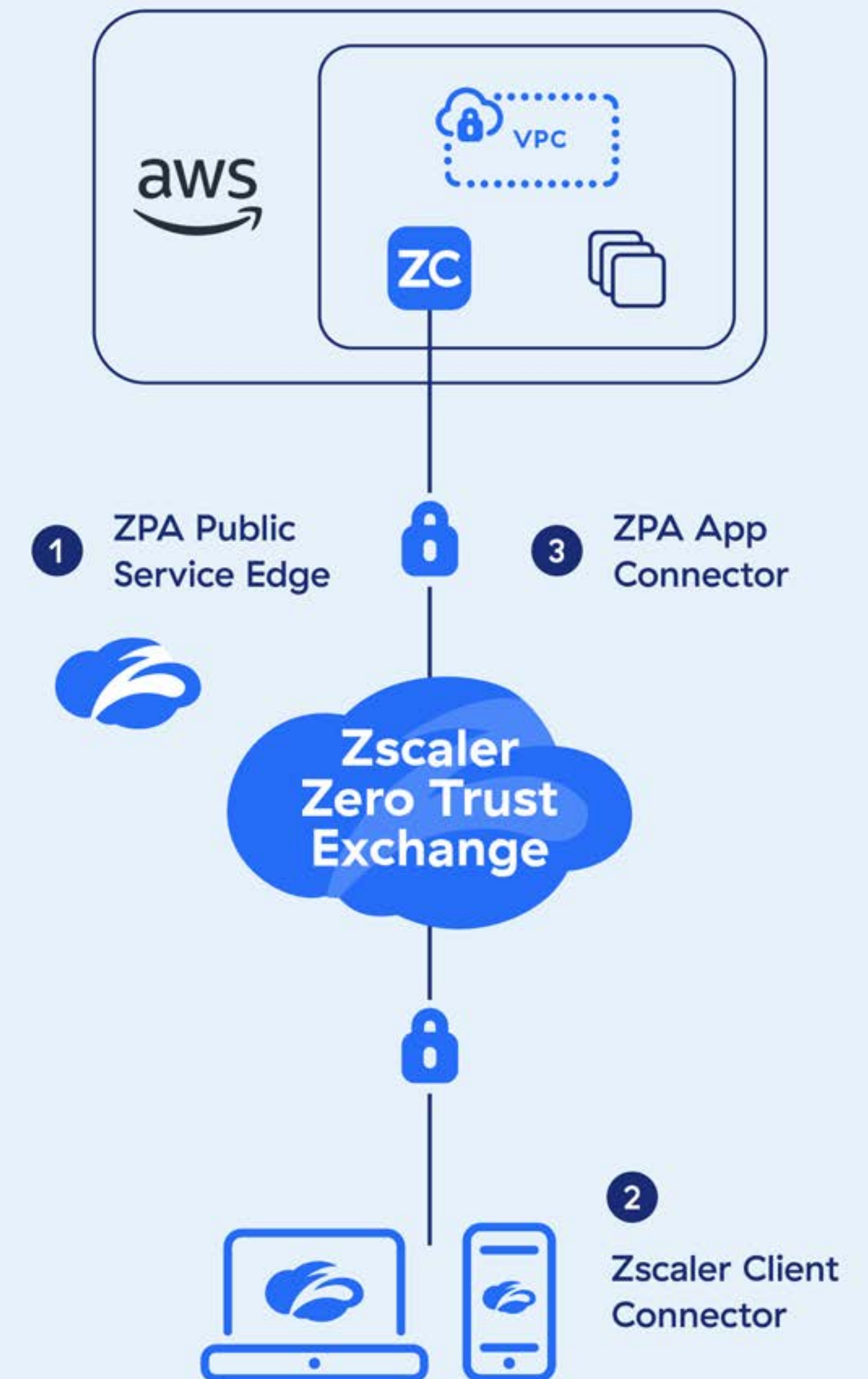
ZIA uses the Client Connector to protect users outside of the corporate network, forwarding Internet traffic through Zscaler's service to ensure a granular security policy.

ZDX uses the Client Connector to perform synthetic probing to a desired Software-as-a-Service (SaaS) application or internet-based service (e.g., Salesforce, Zoom, etc.).

Zscaler clients are quickly and safely moving away from their VPNs...for good. Here's how.

- **ZPA Public Service Edge** hosts policy engine and brokers connections
- **Zscaler Client Connector** endpoint agent forwards traffic to Zscaler cloud
- **ZPA App Connector** connects to private apps and discovers new apps Say goodbye to VPNs. Our clients are moving away from VPNs for good with Zscaler's quick, painless installation.
- IT installs the app connectors onto AWS where applications reside so that Zscaler can reach the apps users will need to access.
- Within the ZPA portal, users define apps and connectors and assign to server groups
- Once installed, the Client Connector can serve multiple purposes: deciding where requests are bound, where they should go, and where to connect users.

Learn more about setting up configuration for the Client Connector.





Ready to transform your
cloud security?

**Zscaler and AWS have paved
the way for the final frontier in
user access, and there's plenty of
room on board.**



Find Zscaler solutions in [AWS Marketplace](#) for simplified
billing and deployment directly on AWS.

Try a free 7-day hosted ZPA demo

In just a few clicks, Zscaler will prepare a report that will supply an
in-depth cloud security posture assessment, showing you where
your vulnerabilities lie on the internet.

[Start your Internet Threat Exposure Analysis.](#)



Act Fast. Stay Secure.

©2026 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, and ZPA™ are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.



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.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at [zscaler.com/legal/trademarks](https://www.zscaler.com/legal/trademarks) are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

[zscaler.com](https://www.zscaler.com)