Zscaler and AWS

Delivering Zero Trust Security for Users, Data, and Workloads

Available in AWS Marketplace

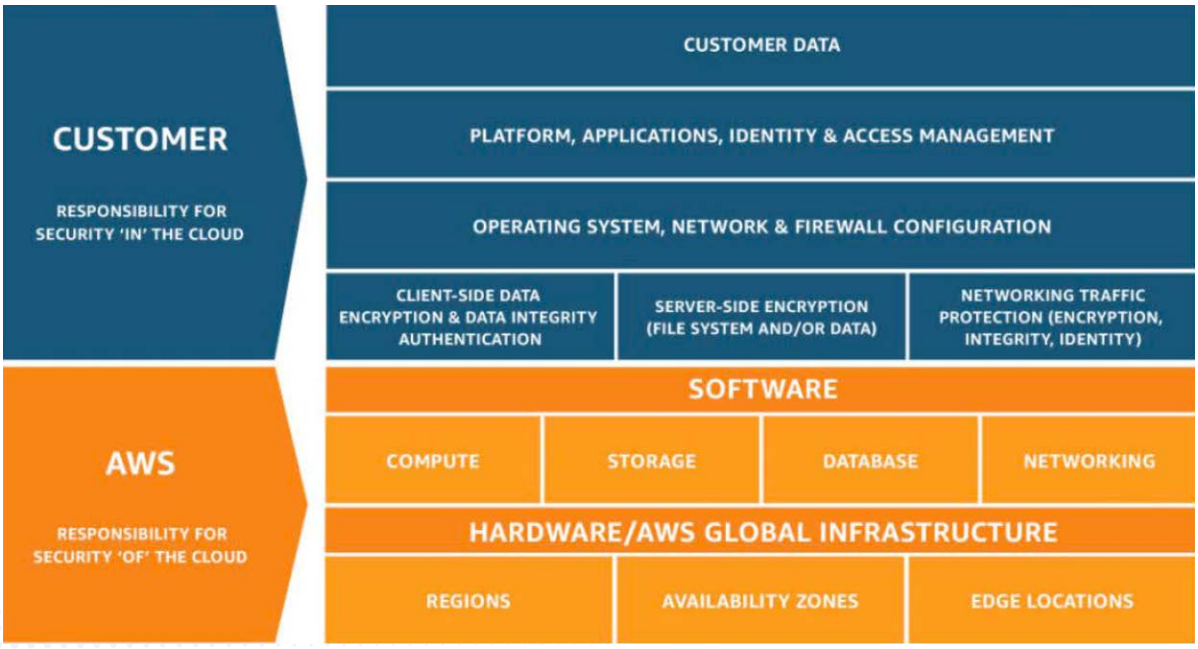
Introduction

Workload migration to Amazon Web Services (AWS) is now a reality for many organizations and public sector agencies. The global pandemic has only reinforced the importance of enterprises accelerating digital transformation and identifying strategies to migrate critical applications to AWS so they can ensure business continuity and resilience, reduce expenses, and gain new efficiencies. IT environments today have evolved from on-premises physical servers to virtualized infrastructure that supports applications and workloads across multiple AWS Regions, enabling users to access these applications anywhere, anytime.

Perimeter-based security has failed to address the needs of modern business

The prevalent security model in the cloud is based on shared responsibility whereby AWS is responsible for the security of the underlying cloud infrastructure while businesses assume the responsibility of securing their workloads and applications in the cloud.

AWS Shared Responsibility Model



Source: https://aws.amazon.com/compliance/shared-responsibility-model/

For the past thirty years, organizations have been building and optimizing complex, wide-area, hub-and-spoke networks, connecting users and branches to the data center over a private network. These hub-and-spoke networks were secured with stacks of security appliances, such as VPNs and firewalls, using an architecture known as castle-and-moat security. This approach served them well when the majority of employees worked at corporate offices with their data and applications residing at the data center.

Today, users work from anywhere and frequently access applications and data that reside in the cloud. For fast and productive collaboration, users require direct access to apps from anywhere at any time. It no longer makes sense to route user traffic back to the data center for access and security in order to reach applications hosted on AWS.

As cyberattacks become more sophisticated and users work from everywhere, perimeter security using VPNs and firewalls provide incomplete, inconsistent security and a poor user experience for the following reasons:

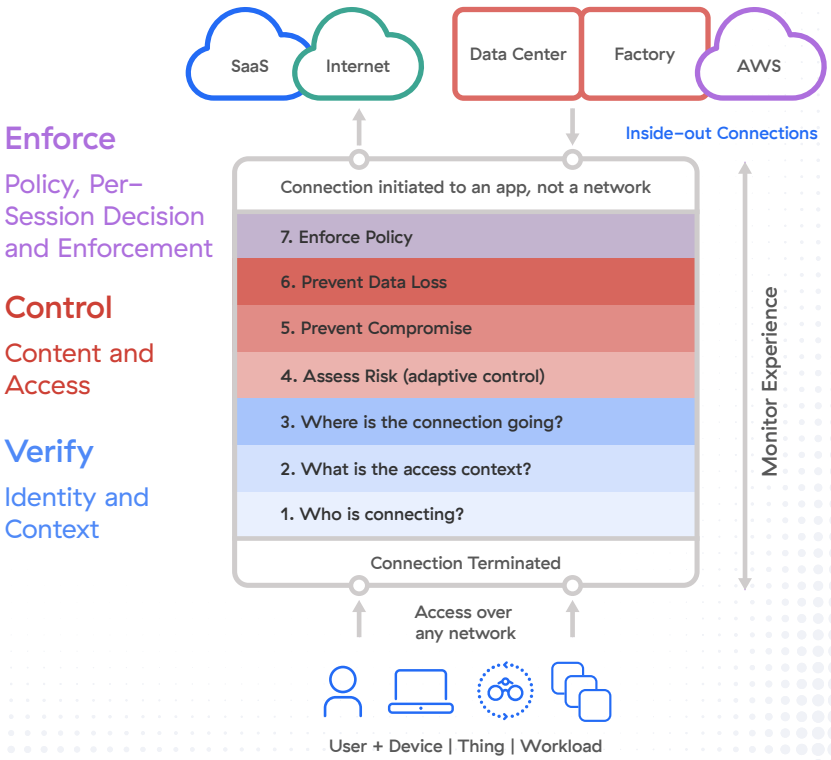
- VPNs and firewalls extend the corporate network, expanding the attack surface and enabling threats to quickly move laterally, resulting in security breaches
- A patchwork of legacy security point products introduces cost and complexity, resulting in missed attacks
- Backhauling remote user traffic to the datacenter for access and security (hairpinning) results in latency, slow performance, and a poor user experience
- Multi-vendor products provide inconsistent security across users, devices, and locations and make it difficult to prioritize threats (multiple dashboards)
- Adversaries bypass traditional defenses with increasingly sophisticated threats delivered at scale
- As organizations undergo application transformation—migrating applications to AWS or embracing SaaS applications—they need to move away from castle-and-moat security based on firewalls and VPNs to a modern architecture that secures fast and direct access to applications from anywhere at any time

They need to adopt a zero trust architecture.

Zscaler Zero Trust Exchange

An AWS Advanced Tier Software Partner, Zscaler has been a leader in zero trust security for a decade and has successfully helped thousands of companies secure their digital transformations with the Zscaler Zero Trust Exchange.

Zscaler's zero trust architecture is an integrated platform that acts as an intelligent switchboard to broker connections between users, devices, and applications in AWS. Every request is verified using identity and context such as device type, location, application, and content. Once identity and context are verified, the zero trust architecture evaluates the risk associated with the connection request, as well as inspects the traffic for cyberthreats and



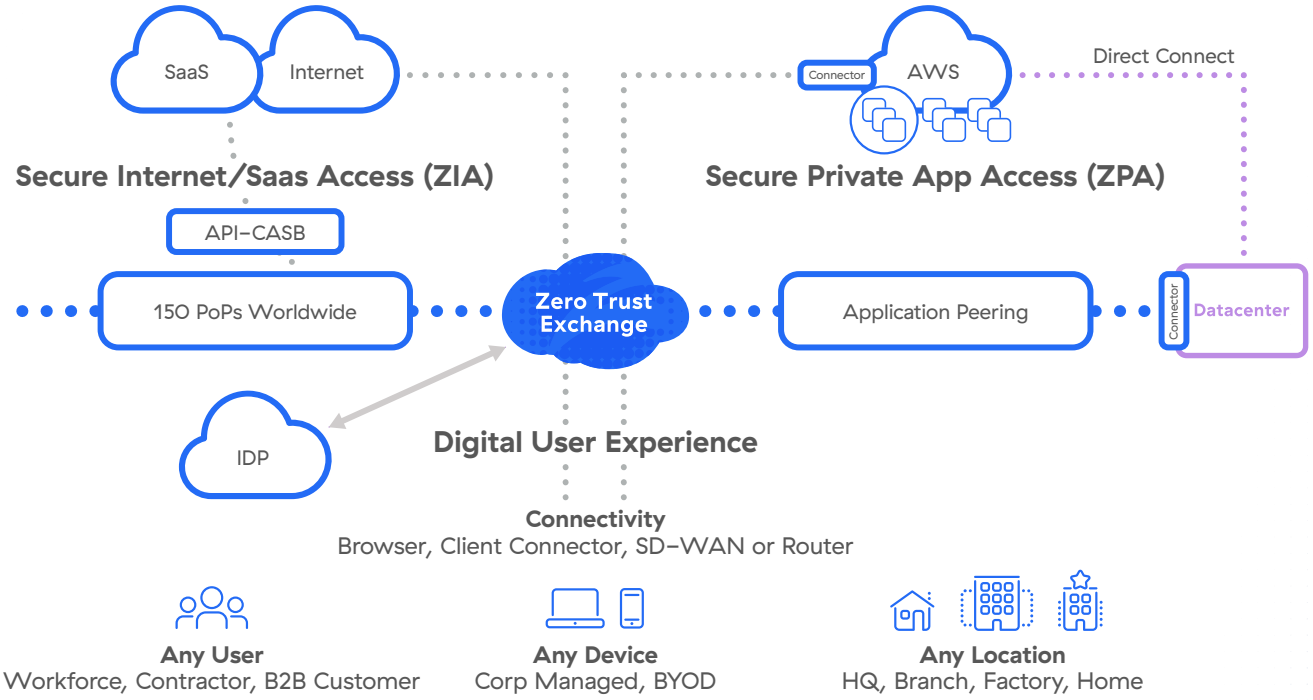
sensitive data. And finally, policy is enforced before establishing a connection to AWS applications. This modern approach eliminates security, networking, and backhauling/performance challenges, enabling organizations to accelerate their app and workload migrations to AWS while delivering superior security and a positive user experience.

The Zero Trust Exchange is the world's largest security cloud with over 150 points of presence (PoPs) around the world and in most AWS Regions globally, including GovCloud East and West. The distributed architecture with performance hubs ensures that any communication can be sent directly to AWS efficiently and securely.

How Zscaler and AWS drive secured digital transformation

1. Protecting the users

Powering a user–focused, secure hybrid workforce requires flexibility for supporting employees and third parties in any location and on any device. It calls for a user experience that offers fast, secure, and reliable access to data, apps, and workloads within AWS. It demands a solution that scales with the business and protects against known and unknown threats.



Zscaler protects AWS users by:

- Connecting the users directly to specific AWS workloads and never to the network. This ensures that threats cannot propagate laterally to infect other users, devices, and applications
- Having users and apps sit behind the zero trust exchange to render them invisible from the internet. Bad actors can't attack what they can't see. As a result, users are not affected by malware or cyber threats such as ransomware and phishing

This enables organizations to significantly reduce risk, improve productivity, and deliver a superior user experience.

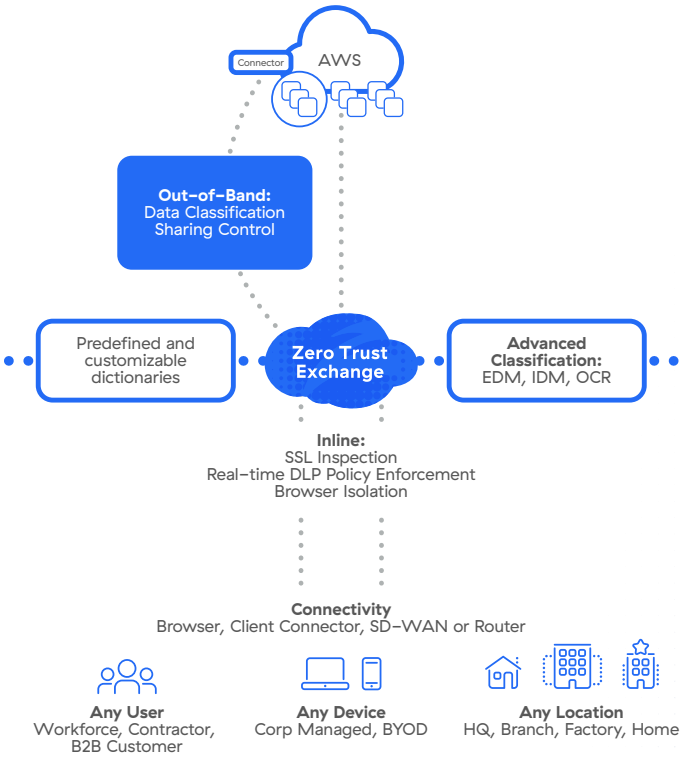
Zscaler is a complete, integrated cloud-native solution that replaces disjointed, legacy point products and fulfills the vision for security service edge (SSE) by bringing together several core technologies to support AWS workloads. These include:

- Zscaler Internet Access (ZIA) for cloud secure web gateway (SWG), cloud access security broker (CASB), cloud data loss prevention (DLP) and more
- Zscaler Private Access (ZPA) for next-gen zero trust network access (ZTNA)
- Zscaler Digital Experience (ZDX) for digital experience monitoring (DEM)

2. Protecting the data

Users work remotely from a variety of devices, accessing and uploading data in AWS offerings like S3. As a result, perimeter-focused security appliances cannot protect this data, and turning to a different point product for each new use case breeds cost and complexity.

Zscaler Data Protection follows data wherever it goes to enforce the principles of zero trust. Data is scanned inline for real-time classification and policy enforcement. Browser isolation streams data as pixels to unmanaged devices to stop exfiltration. Data at rest in AWS is scanned for sensitive information and automatic revocation of risky shares.



Zscaler Data Protection is set apart by:

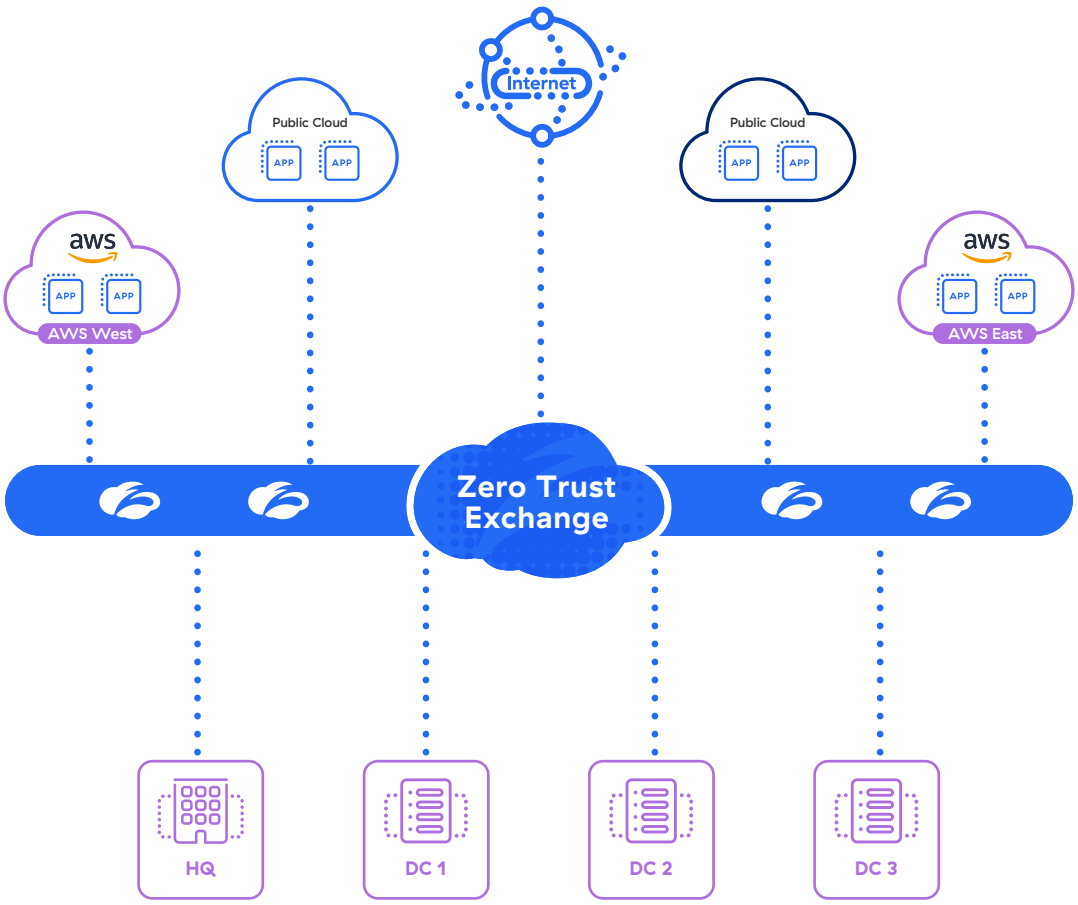
- Being part of the most unified security platform that fills the needs of SSE and beyond
- A unified policy engine that protects data consistently wherever it goes
- Full SSL inspection from the world's largest, most high performance security cloud
- A proven platform deployed at scale across the world's largest organizations

3. Protecting the workloads

As workloads migrate to the cloud, organizations have an urgent and compelling need to modernize their networks and security to ensure business competitiveness. Legacy architectures, using VPNs, firewalls and security virtual appliances create routable mesh networks which expand the network attack surface and increase the risk of workload compromise. Complexity increases as multiple virtual appliances are replicated across locations. This creates significant challenges for organizations such as the risk of lateral threat movement, reduced productivity and collaboration as well as higher costs and the complexity of managing network security architectures to secure a hybrid workforce and cloud-based applications.

Zscaler has extended its proven Zero Trust Exchange to secure not only user traffic, but hybrid and multi-cloud connectivity with Workload Communications. The solution enables a specific workload to securely communicate with another workload in any region of any cloud provider, over any network — often over the internet in both hybrid and multi-cloud environments. This consolidated approach not only eliminates the need to acquire and manage point product solutions that increase cost and management overhead, it also increases cross-functional collaboration between teams and accelerates digital transformation.

Workload Communications



With Workload Communications, Zscaler has completely reimagined cloud connectivity by enabling zero trust for cloud workloads which delivers simple, secure access for workloads to the internet and private applications. Unlike legacy network solutions, Workload Communications provides a direct-to-AWS architecture using the proven Zscaler Zero Trust Exchange platform to verify trust based on identity and context to enable secure workload-to-internet communication, workload-to-workload communication across multiple regions and AWS Availability Zones and workload-to-workload communications within the AWS environment.

Workload to Internet

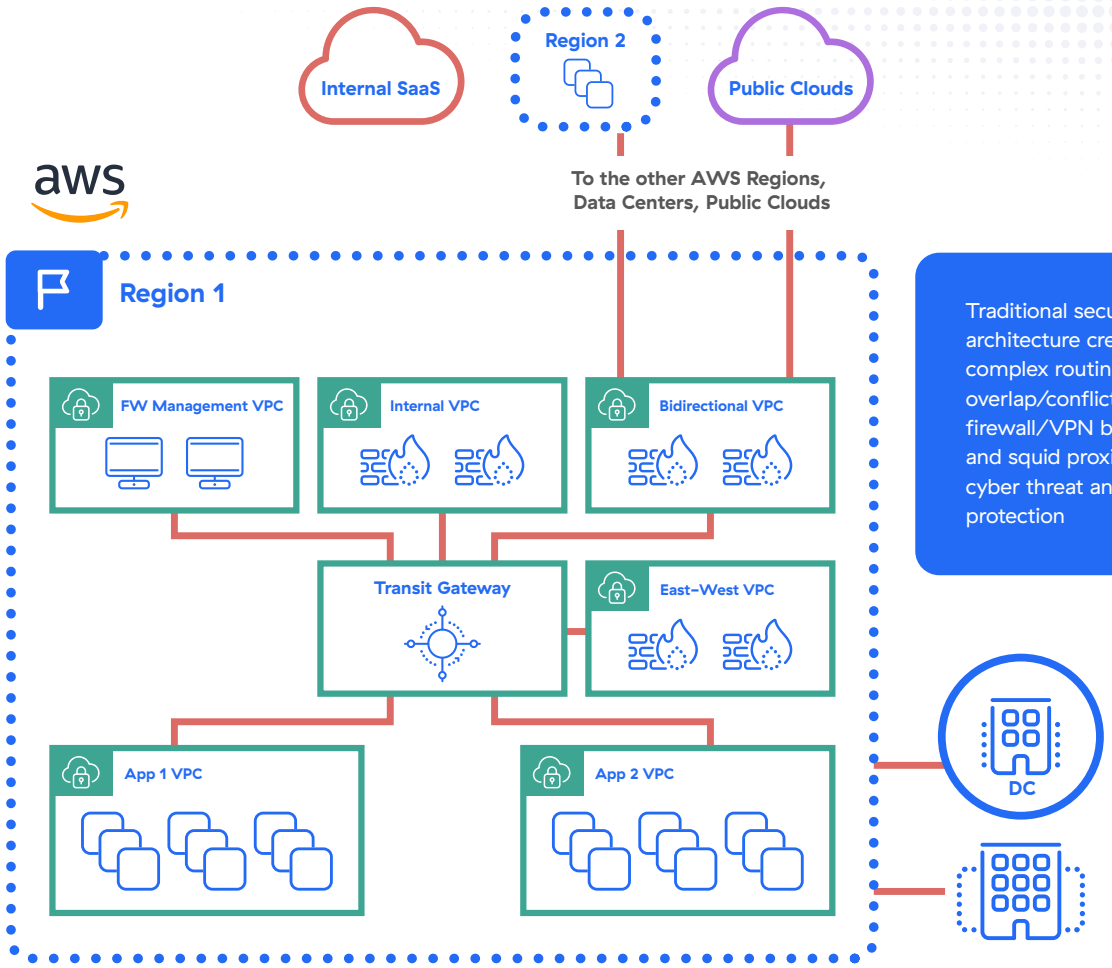
- Attack surface reduction
- Runtime compromise and data loss prevention without virtual FWs/proxies

Workload to Workload

- AWS accounts
- AWS to data center

Segmentation

- User-to-app, app-to-app segmentation without network segmentation
- AWS workload identity based micro-segmentation

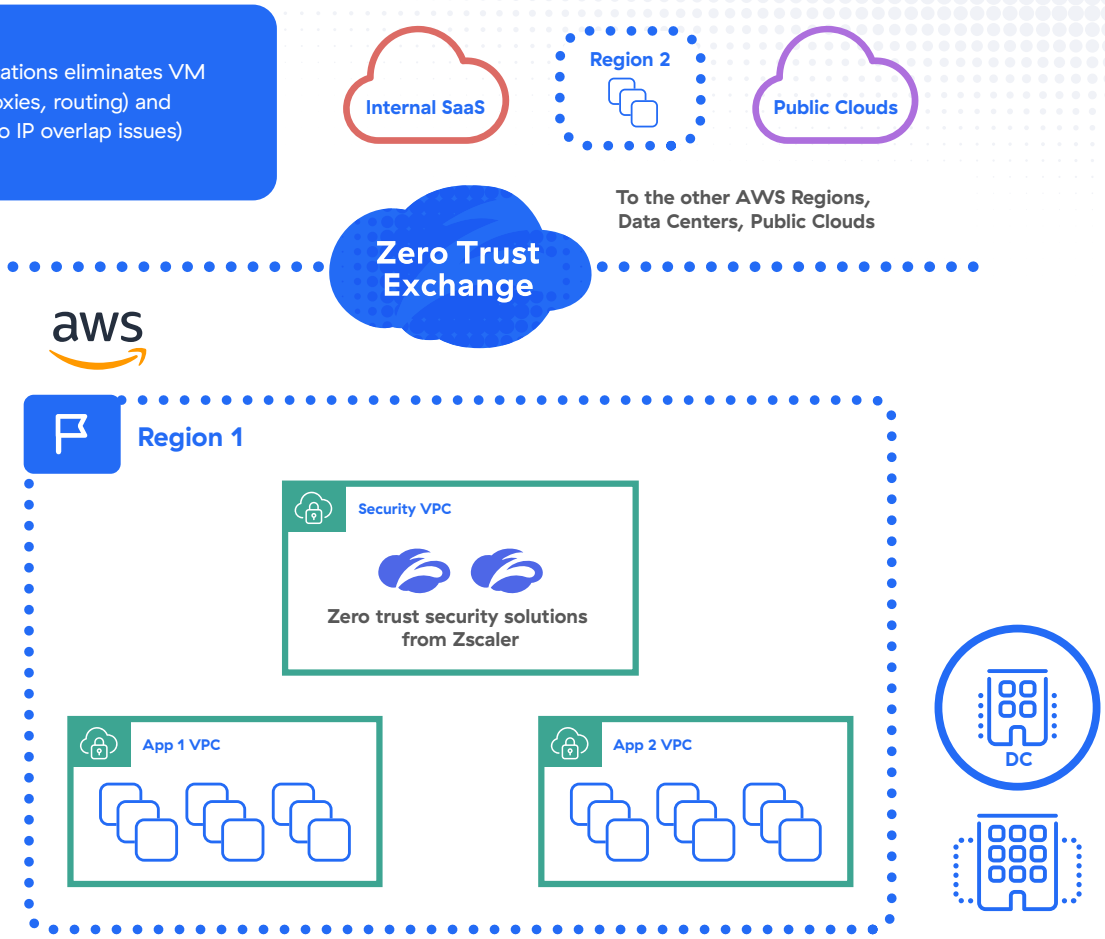


Key Benefits

Workload Communications eliminates the network attack surface by directly connecting workloads to the internet and to private applications using a full proxy architecture. This architecture dramatically simplifies connectivity by eliminating routing, VPNs, transit gateways, transit hubs, and firewalls, while allowing for flexible forwarding and easing policy management by using the proven ZIA and ZPA policy framework. This unique approach provides three key benefits to AWS users:

- Zero attack surface and data loss prevention – By using direct-to-cloud architecture to take traffic off the corporate network, applications in AWS environments are invisible to cyber threats reducing the risk of data loss
- Simplified cloud connectivity – The Zero Trust architecture also avoids performance bottlenecks as IP overlap issues are removed, route distributions are no longer needed, and workloads are directly connected to other applications
- Superior application performance at scale – Zscaler is built on a truly distributed architecture where every communication that reaches the service edge gets processed instantly for identity and context. The peering relationship with AWS in most regions globally, including GovCloud East and West ensures the shortest path between applications no matter where they are hosted, reducing latency and improving application performance

Workload Communications eliminates VM bloat (FWs, squid proxies, routing) and routing complexity (no IP overlap issues)



Summary

Together, Zscaler and AWS are helping organizations drive their secured digital transformation journeys, delivering:

- Efficient routing that reduces latency and accelerates workload migration to AWS
- Network and security architecture simplification via the elimination of firewalls and VPNs
- Always-on access that improves end user experiences
- Stronger, more comprehensive security posture to eliminate threats to cloud native applications
- Increased business agility for a competitive edge
- Lower costs to free up funds that are better spent elsewhere in the business

Zero trust security solutions from Zscaler are readily available for purchase on the AWS Marketplace. We have everything you need to protect your users, data, and workloads.

Learn more about Zscaler for AWS

zscaler™ | Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

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