



Workload Communications: Modern zero trust security for cloud workloads on AWS



Challenges


Legacy network security is inadequate for cloud workloads


As organizations move away from on-premises physical servers to virtualized infrastructure residing in the cloud, they face new challenges. Traditional networks and legacy castle-and-moat security (VPNs, firewalls) were never designed for the cloud, resulting in poor security, slow performance, and an expanded attack surface. And when deploying workloads in mixed environments with multiple cloud providers, the mesh network that connects workloads becomes costly and difficult to implement, scale, and manage.

To accelerate digital transformation, organizations must efficiently migrate all workloads, including critical applications, to the cloud to ensure business continuity, gain new efficiencies, and reduce costs.

Benefits

Zscaler Workload Communications provides industry leading¹ zero trust security and simple, secure access for workloads to the internet, private apps, or public clouds

-  **Eliminate lateral threat movement**
- Direct-to-cloud architecture ensures
- least privilege access for cloud workloads
- and applications, taking traffic off the
- corporate network and preventing lateral
- threat movement.


-  **Reduce operational cost and complexity**
- Eliminates IP overlap issues, route distributions, and costly legacy point products (VPNs, firewalls, etc.).
- Provides automated deployment and consistent security for all workloads.

The Zscaler Solution

Zero trust security with operational simplicity to protect cloud workloads

Zscaler Workload Communications enables organizations to reduce their attack surface and eliminate lateral threat movement by utilizing an industry leading zero trust architecture. By forwarding all workload egress traffic to the Zscaler Zero Trust Exchange, consistent security policies and access controls are applied along with full inspection of TLS/SSL traffic. Workload traffic is then directly forwarded to its destination, including the internet, SaaS applications, or other workloads hosted in other regions or data centers.

Zscaler eliminates the cost and complexity of legacy VPNs and firewalls, while providing flexible security and policy management, along with consistent protection against threats and data loss.



-  **Consistent threat and data protection**
- Prevent zero-day attacks and protect data
- with cloud-scale TLS inspection, segmentation
- (across regions, public clouds), advanced
- threat protection, and data loss prevention.

¹Gartner: Magic Quadrant for Security Service Edge (SSE), April 10, 2023

Zscaler on AWS

The Zscaler Zero Trust Exchange is the world's largest inline security cloud, built on AWS, and it protects thousands of AWS customers. Zscaler securely connects users to workloads, workloads to workloads, and devices to devices with over 150 PoPs globally and in most AWS regions, including GovCloud East and West. The Zscaler Zero Trust Exchange has completely reimagined workload communications to deliver simple, secure access for workloads to the internet, private apps, on-premises data centers, and multiple public clouds including AWS.

Features

-  **Eliminate lateral threat movement and reduce the attack surface**
 - Zscaler Workload Communications provides a direct-to-cloud architecture using the industry leading Zscaler Zero Trust Exchange platform to deliver zero trust connectivity that works over the internet and AWS Direct Connect. By never putting users, apps, or workloads on the corporate network, threats cannot move laterally. And placing apps and workloads behind the Zero Trust Exchange makes them invisible to threats, reducing the attack surface.
-  **Consistent threat protection and superior performance**
 - The Zscaler platform inspects all traffic inline to protect against cyberthreats and data loss, establishes the identity and context of the access request, and applies all appropriate policies before establishing connectivity to the internet, SaaS apps, or private workloads. With over 150 PoPs worldwide, Zscaler ensures the shortest path no matter where workloads are hosted. This eliminates traffic backhauling, reduces latency, and provides fast application and workload performance.

Case Study: Multinational industrial manufacturing company

Challenges

- High costs and complexity from managing 10k+ workloads across 1k+ cloud accounts with traditional network security products
- Inconsistent security policies across different cloud infrastructures and managed cloud applications
- Slow performance due to backhauling traffic from public clouds to data centers for security

Solution

Zscaler Workload Communications enabled the organization to achieve their key objectives, including secure workload access to the internet and private applications across their multi-cloud environment

Results

Stronger security: all internet-bound workload traffic, encrypted and unencrypted, is inspected with consistent security policies

Simplified connectivity: direct-to-internet and multi-cloud connectivity via the Zero Trust Exchange eliminated backhauling

Scalability: global Zscaler presence to support 10,000+ workloads in AWS

Reduced cost and complexity: by eliminating legacy security products and utilizing a centralized control plane

Obtain Zscaler solutions on the [AWS Marketplace](#) and learn more at the [Zscaler website](#) today.

 | 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 SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at [zscaler.com](#) or follow us on Twitter [@zscaler](#).

©2024 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™, Zscaler Digital Experience™, and ZDX™ 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.