Zscaler™ Workload Protection at a Glance

Benefits:

Zero Attack Surface

Protect applications from compromise by removing the need for the corporate network to facilitate outbound communications—thus eliminating the network attack surface and lateral threat movement.

Prevent Data Loss

By taking workload communications off the corporate network and enabling direct communications, intercepting workload data is averted and bad actors can no longer move laterally to access crown jewel data.

Simplified Cloud Connectivity

Avoid legacy networking complexity and challenges with a zero trust architecture that decouples workload security and communications from the network across any cloud or data center.

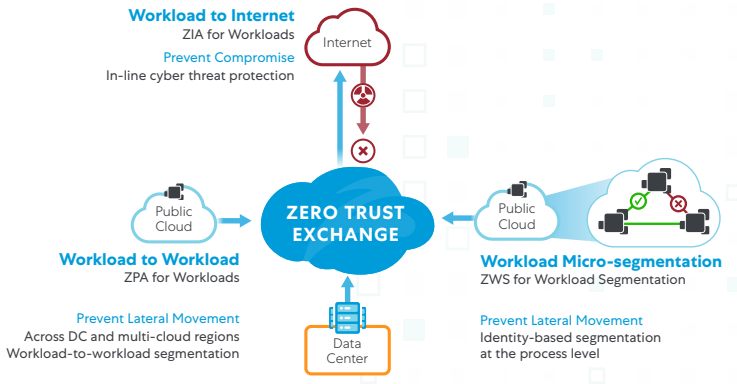
Superior Application Performance

Minimize latency and eliminate performance bottlenecks with the Zscaler Zero Trust Exchange which is purpose-built for scale with more than 150 points of presence (POPs) distributed globally.

Overview

Workload migration to the cloud is now a reality for many organizations. The Covid-19 pandemic has only reinforced how important it is for organizations to accelerate digital transformation and identify strategies to migrate all workloads, including critical applications, to the cloud to ensure business continuity, build resilience, save costs, and gain new efficiencies. Modern data center infrastructures have evolved from on-premises physical servers to virtualized infrastructure that support applications and workloads across multiple cloud environments. Ensuring effective workload communications across hybrid and multi-cloud environments has become a foundational requirement as organizations transition to the cloud. However, most of them still rely on traditional IP and firewall-centric solutions to extend their network and apply perimeter-based security to execute their cloud strategy. While this approach served them well when their applications resided in their data centers, it creates security, network, and application performance challenges in a cloud-first world. Additionally, as organizations accelerate their cloud journey and begin to deploy workloads in multiple regions with multiple cloud providers, the mesh network used to connect all the workloads becomes increasingly costly and difficult to implement, scale, and manage.

With Workload Protection, 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 Protection provides a direct-to-cloud architecture using the proven 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 clouds (whether public and private), and workload-to-workload communications within an environment. Workload Protection delivers a network-agnostic zero trust fabric that works over the internet andDirect Connect and ExpressRoute that work to eliminate cybersecurity risk, prevent data loss, simplify cloud connectivity, and provide improved application performance at scale.



Workload Protection Key Capabilities

Cost Effective Cloud Connectivity

Eliminate the need to provision and manage VPN/MPLS connections between clouds and on-premises environments. Instead, establish inside-out DTLS connections across multi- and hybrid-cloud environments, brokered through the Zscaler Zero Trust Exchange.

Secure Cloud Egress Controls

Workload Protection takes an allowist approach and enables granular identity and location-based egress controls for cloud applications communicating with internet services. In addition, centralized policy management enforces consistent and standardized security policies across all cloud environments.

Complete Visibility and Reporting

Workload Protection provides granular audit-compliant logging of all forwarded application traffic and its associated access information. In addition, it supports Nanolog Streaming Service (NSS) to stream all logs to the customer's SIEM in real-time automatically.

Part of the World's Largest Security Cloud

Workload Protection leverages the proven scale, performance, and reliability of the Zero Trust Exchange to ensure safe, controlled access from any cloud, with no exposed attack surface.

Granular Access Controls

Workload Protection provides identity-centric application policies to control access between applications, cloud services, and workloads. Access control policies use location and DNS attributes and remain agnostic to network information. Workload Communication policies support the flexible steering of forwarded traffic to other clouds and to the internet.

Friction-Free Deployment

Zscaler's Workload Protection allows zero-touch deployment and automated policy configuration through deep integration with cloud-native services and automation tools. It can be auto-deployed across multiple clouds within minutes.

zscaler™

To learn more about what Zscaler Digital Experience can do for you go to **zscaler.com/cloudconnectivity**

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com