DATA SHEET

Zscaler Workload Protection

Zscaler Workload Protection enables simple, secure access for workloads to the internet and to private applications, in public and private clouds, with a direct-to-cloud architecture.

As workloads migrate to the cloud, organizations have an urgent and compelling need to modernize their networks to ensure business competitiveness. Legacy network-centric architectures, which were designed for static environments, simply cannot handle cloud connectivity needs, especially in a multi-cloud world. As a result, the attack surface expands, and operational complexity increases.

For organizations that are modernizing their infrastructure, ensuring effective and secure workload communications should be a foundational requirement. The Zscaler Zero Trust Exchange has completely reimagined workload communications to deliver simple, secure access for workloads to the internet and private applications. Unlike legacy network security, Workload Protection uses a direct-to-cloud architecture, which is built on the proven Zero Trust Exchange platform. Customers gain numerous benefits including better security, simpler operations, increased visibility, higher availability, improved application performance, and lower costs after adopting Workload Protection to transform their networks.

Workload Connectivity Challenges With Legacy Network Security

When organizations attempt to connect workloads to the internet or to their other applications in public cloud or data center environments, they face a number of challenges when using legacy network and security architectures, including:

Increased cyber risk, especially with lateral threat movement, from using legacy network-centric connectivity solutions such as cloud VPNs, site-to-site VPNs, firewalls, or WAN technologies, which overextend a customer's trusted network across the internet to other clouds and on-premises environments–this approach increases network attack surface. A patchwork of vendor security virtual appliances, tools, and non-standard policies adds to security risks because of gaps in security coverage that are both known and unknown, all of which invariably leads to potential data loss for an organization by bad actors.

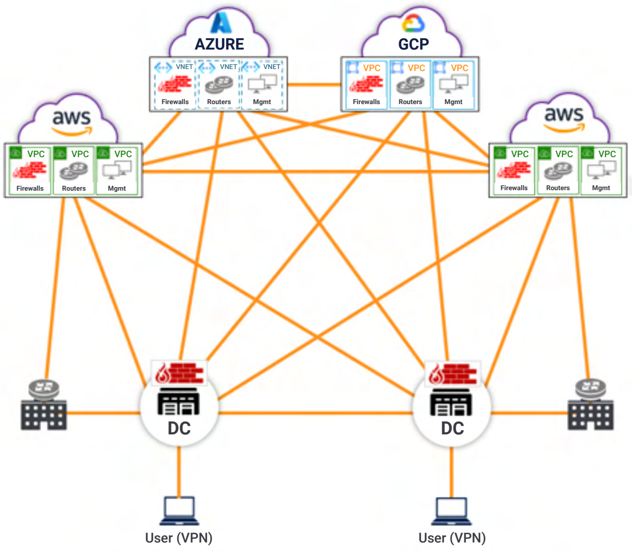
Escalating complexity due to complicated route filtering, multiple network hops, virtual appliances for networking and security, and fragmented policy management from introducing these legacy models to the cloud. And as product development and delivery becomes more agile, continuous, and service-oriented, reining in this complexity is a difficult task for security teams as they struggle to enforce standardized workload connectivity and security policy across multi- and hybrid-cloud environments.

Lack of visibility across the application connectivity paths creates network and security blind spots. Cloud workloads have become more distributed and environments have increased in scale. Connecting these distributed workloads requires obscure multi-hop networks and "daisy chaining" with multiple network and security appliances. This complex connectivity and lack of centralized logging leave operators blind to application communications.

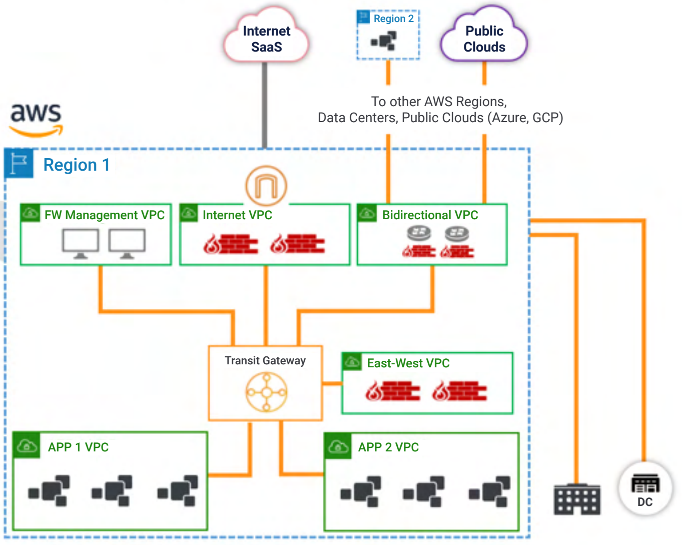
Poor performance and scalability due to legacy approaches being applied to cloud connectivity. Legacy architectures typically use separate VMs for each security function, resulting in sequential assembly line style inspection resulting in increased latency. These architectures also cannot scale fast enough to meet the demands of surges in traffic.

High costs due to legacy network security appliances (e.g., firewalls, IPS, routers, and other point products), overprovisioning of network services to compensate for lack of scalability, and increased use of cloud-native services such as transit peering.

Extend the Corporate WAN to the Cloud
Single infected workload infects entire network



Adapt Network Security to the Cloud
Complex routing, IP overlap/conflict
FW VM bloat and squid proxies for cyber threat, data protection



Workload Protection extends zero trust principles to cloud workloads

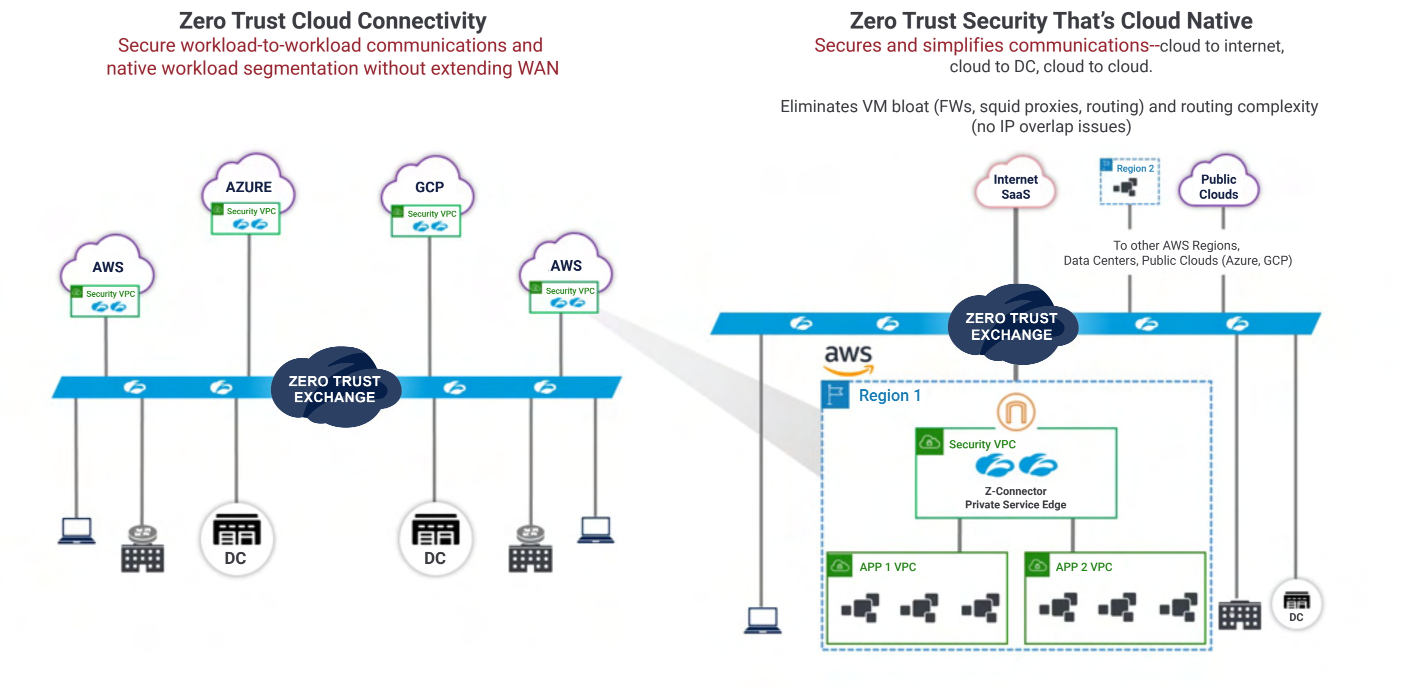
Workload Protection provides workloads fast and reliable access to the internet and private applications with a direct-to-cloud architecture, which provides high security and operational simplicity. Workload Protection eliminates the network attack surface by directly connecting workloads to the internet 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.

The unique direct-to-cloud architecture is made possible by using the Zero Trust Exchange. Workload Protection directly forwards all workload communications to the Zero Trust Exchange, where either ZIA or ZPA policies can be applied for full security inspection and access identity-based control of workload communications. From the Zero Trust Exchange, the communications are then forwarded to any destination, whether it's the internet or other private applications within or across multi-cloud environments. This unique approach provides three key advantages:

- **Zero attack surface and data loss prevention** – By using direct-to-cloud architecture to take traffic off the corporate network, applications become 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 the internet 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 ensuring the shortest path between applications no matter where they are hosted, reducing latency and improving application performance.

Workload Protection is well-aligned to help an organization meet its infrastructure modernization priorities in several ways. It extends workload-to-workload connectivity, using zero trust principles, across disjointed networks and multiple clouds, including AWS regions, Microsoft Azure, Google Cloud, and on-premises data centers. Workload Protection also delivers secure internet access for workloads in public clouds and data centers. All these capabilities are delivered via a unified policy plane for traffic forwarding, security, and zero trust access across these heterogeneous environments.



Zero Trust Cloud Connectivity

Secure workload-to-workload communications and native workload segmentation without extending WAN

Zero Trust Security That's Cloud Native

Secures and simplifies communications--cloud to internet, cloud to DC, cloud to cloud.

Eliminates VM bloat (FWs, squid proxies, routing) and routing complexity (no IP overlap issues)

Workload Protection advantages

- **Zero trust security for workloads.** As described above, workloads benefit from zero trust security which is based on workload identity, location, and other contextual attributes, unlike traditional controls which rely on networks for security.
- **Simpler deployment, without complicated network configurations.** Traditional approaches require complex routing configurations through transit gateways, transit hubs, and SNAT which need to be repeated for every VPC and across every cloud. In contrast, all that Workload Protection needs is a default route to the internet. Policy management for traffic forwarding and security is centralized and standardized in the Zero Trust Exchange regardless of the source or destination of the workload communications.
- **Full visibility, end to end, with direct-to-cloud connectivity.** The old way relies on obscure, multi-hop networking making it difficult to understand how traffic flows. Moreover, logging is scattered across multiple network products. Because Workload Protection connects directly to the cloud, operators gain full visibility and control over how workloads communicate. Logging is centralized and streamed in real time, and logs can be exported to a SIEM or a monitoring solution of your choice for correlation and analysis.

- **Hyper scalability and performance**, with no centralized chokepoints. Legacy architectures require all traffic to be funneled through centralized infrastructure, involving transit gateways, hubs, and virtual firewalls which lack the elasticity and scale to handle surge throughputs. The modern Zero Trust Exchange architecture operates at hyperscale across more than 150 global data centers and handles any increase in communications with elastic, horizontal scaling. Furthermore, Zscaler's single-pass architecture reduces hops and the associated latency to improve application performance.
- **High availability without unnecessary replication of services.** Existing approaches require a complex availability architecture of multiple firewalls and networking configurations that need to be replicated over multiple zones, regions, and clouds. The Workload Protection direct-to-cloud architecture dramatically simplifies cloud configuration requirements because all the required services are transparently provided in the Zero Trust Exchange, at scale. At the customer's site, automatic failover with N+2 redundancy is provided for forwarding and security.
- **Reduced costs with streamlined services delivered by the Zero Trust Exchange.** Customers no longer have to overprovision services and pay for idle time of firewalls, transit hubs, and NAT gateways replicated across every cloud environment, which quickly add up. With Workload Protection, there are no hidden costs, and customers are only billed for consumed security services, not for networking or access—there is no need to pay for virtual firewalls or proxies in the customer environments.

Workload Protection unique value

Workload Protection is built on the Zscaler Zero Trust Exchange, which securely connects users, devices, and apps using business policies over any network and across any cloud, at scale.

- Application workloads are connected directly to each other, independent of the underlying corporate network, VPN, or WAN
- Applications are invisible to the outside world and have no attack surface
- Purpose-built, multi-tenant proxy architecture holds, inspects, and enforces policy
- High-performance inspection is done by a single-scan and multi-access architecture that is built for scale
- Fine-grained forwarding policy management for internet & non-internet traffic, using Zscaler Internet Access or Zscaler Private Access policies
- Unified, standardized policies across AWS, Azure, Google Cloud, and on-premises data centers. This includes managing policy, monitoring traffic, and tracking logs

Workload Protection use cases

Digital transformation and cloud migration

As organizations migrate their applications to the cloud and build cloud-native applications, the on-premises models for networking and security get broken. Digital transformation necessitates a network transformation, which ushers in a new model for workload communications; a model in which workloads communicate with any destination securely and independently from the underlying network. Workload Protection is purpose-built to enable digital transformation.

Workload connectivity without VPNs

Organizations can now directly connect workloads to private applications without extending their WAN or relying on VPNs, both of which increase network attack surface.

Ransomware and malware prevention with zero trust

Zero trust assumes that the network has been compromised and can no longer be trusted. In this scenario, Workload Protection directly connects workloads to the internet or to private applications without connecting networks. As a result, the network attack surface is eliminated and threats, such as ransomware, cannot spread laterally across the environment. Every connection is monitored and logged for audit purposes.

Securing cloud workload access to the internet

Workloads can be considered a mirror image of users. Just like users, workloads can be directly connected to the cloud via ZIA and benefit from the same policy framework, security inspection, and access control. Virtual firewalls are not required.

Mergers and acquisitions

Merging two disparate networks is incredibly challenging and time-consuming. Problems range from IP overlaps, to routing issues, to increased security risk from an enlarged network attack surface when two networks are combined. With Workload Protection, networks do not need to be merged—they can be kept separate, and workloads from one environment can surgically connect to private applications in another environment quickly and without disruption.

Capabilities fact sheet

Zero touch provisioning and automated deployment

- Zero touch provisioning with system-defined templates for AWS and Azure
- Fully automated deployment (AWS CloudFormation, Azure Resource Manager Templates, and Terraform)
- Dynamic discovery of customers Geo-regions, Availability zones, VPC/VNETs
- Built-in SLA monitoring and failover
- Available on AWS and Azure marketplaces

Granular forwarding policy for internet and non-internet traffic

- Options to send the traffic to ZIA, ZPA, or Direct (bypassing Zscaler services)
- Flexible traffic selection criteria location, sub-location, location group, 5 tuple or FQDN
- Built-in availability with seamless failover to next available service pop

Unified policy for forwarding and security with Workload Protection and ZIA

- Locations are created dynamically for the VPCs/VNETs
- Dynamic Workload Protection locations are synced into the ZIA platform
- Locations created by Workload Protection are like any other existing ZIA location. Any and all security policy can be enabled, including IPS, SSL proxy, URL filtering, and data protection

Unified zero trust policy for user-to-server and server-to-server

- ZPA delivers a unified policy for user-to-application and server-to-server
- Existing ZPA policy is enhanced to include new client type (Workload Protection) to support server-to-server connectivity
- Workload Protection groups created for forwarding traffic in AWS, Azure, and the data center are synced to the ZPA platform

Unified policies, control, and management across AWS, Azure, and branch connectors

- Cloud-delivered and centralized dashboard for device health and traffic monitoring
- Filtering available for Azure, AWS, and branch deployments
- Time series for flow count & byte count for ZIA, ZPA, Direct, DNS

Consolidated logging infrastructure for all types of traffic

- Detailed session logs covering traffic going to ZIA, ZPA, and direct (Zscaler bypass)
- All DNS transactions are logged for both public and private DNS
- Fully integrated with NSS infrastructure—existing NSS firewall VM can be used to stream the logs to SIEM

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