Data Sheet

Zscaler Workload Communications

Zscaler Workload Communications secures workload-to-Internet, multi-cloud and multi-region traffic for your mission-critical cloud workloads with the power of the Zscaler Zero Trust Exchange™.

Public cloud adoption enables digital transformation at scale, driving a massive influx in cloud-based workloads hosting sensitive communications and data with SaaS applications or workloads in multiple public clouds or data centers.

As a result, securing these mission-critical workloads is vital for enterprises to ensure their continued success and protect sensitive data. However, legacy architectures are inadequate to secure public cloud workloads, amplifying lateral movement, increasing operational complexity and cost and creating inconsistent threat and data protection.

Zscaler radically simplifies cloud workload security with Workload Communications. It secures workload-to-Internet, multi-cloud and multi-region traffic for your mission-critical cloud workloads with the power of the Zscaler Zero Trust Exchange™

Workload Communications effectively provides zero trust security that eliminates lateral movement, reduces operational cost and complexity, and ensures consistent threat and data protection.

> “With Zscaler’s Workload Communications, we can easily standardize security policies for both users and applications regardless of where they are located.”
>
> **Rui Cabeço,** Global Outbound Connectivity Lead, Siemens

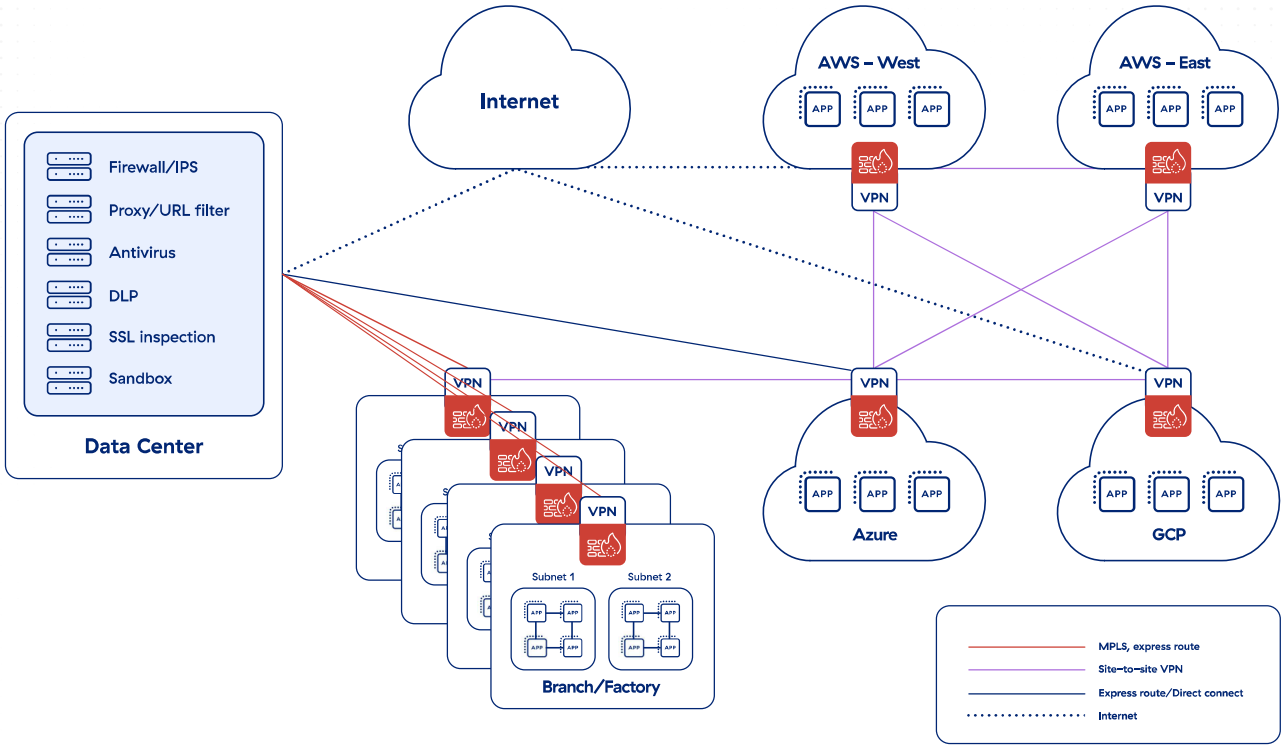
Challenges with legacy cloud workload security

Many enterprises rely on legacy security architectures to secure their cloud workloads. Many will use a combination of:

- Native security solutions offered by public cloud service providers
- Third-party tools (firewall, VPN, TLS/SSL inspection, DLP, etc.) for extra layers of protection
- Legacy on-premises network security infrastructure for inspection and protection

However, several challenges arise from this architecture, including:

- **Increased lateral threat movement and cyber risk.** Network connectivity and security solutions such as site-to-site VPNs and firewalls extend the network to cloud workloads, amplifying lateral movement risks. Additionally, each internet facing firewall increases the attack surface. This can span the internet to different clouds and on-premises environments. Additionally, a patchwork of virtual appliances, operational tools, and nonstandard policies adds to security risks because of both known and unknown gaps in security coverage.
- **Increased complexity and poor performance.** Legacy network and security solutions were not built with cloud workloads in mind. Site-to-site VPNs need to be created. Numerous point products, such as Virtual Firewalls, Proxies, NAT Gateway, must be incorporated. Additionally, some solutions may use separate VMs for each security function, resulting in sequential assembly line style inspection and thus increased latency. This creates significant operational complexities when applied across multicloud.
- **High costs.** Use of legacy network security point products (e.g, firewalls, IPS, routers, etc.), overprovisioning of network security infrastructure to compensate for lack of scalability, and increasing use of cloud native services all contribute to increased capex and opex.
- **TLS visibility gaps.** TLS inspection often comes with increased compute resources and can pose challenges such as performance degradation when enabled. Managing distributed certificates or applying exclusions to pinned workloads creates operational challenges. Additionally, it often leads to increased costs in terms of cyber security infrastructure to support scale.
- **Lack of Common Logging.** Legal and regulatory requirements require organizations to store logs for an extended period of time. Getting access to these logs from different cloud environments and storing them in a central SIEM infrastructure can be complex and expensive.



Workload Communications extends zero trust architecture to cloud workloads

Workload Communications eliminates the network attack surface by connecting workloads to the internet and private applications using zero trust architecture. This dramatically simplifies connectivity by reducing your organization's dependency on site–to–site VPNs, and firewalls while allowing for flexible forwarding and easing policy management with the proven ZIA and ZPA policy framework.

This is all made possible by the Zscaler Zero Trust Exchange. Workload Communications directly forwards all workload egress traffic to the Zero Trust Exchange, where security policies can be applied for full TLS/SSL inspection and access control. Workload traffic is then forwarded to its intended destination, whether it's the internet, SaaS applications, or other workloads hosted in other public clouds or data centers.

With Workload Communications, can help you will benefit from:

Eliminating Lateral Movement

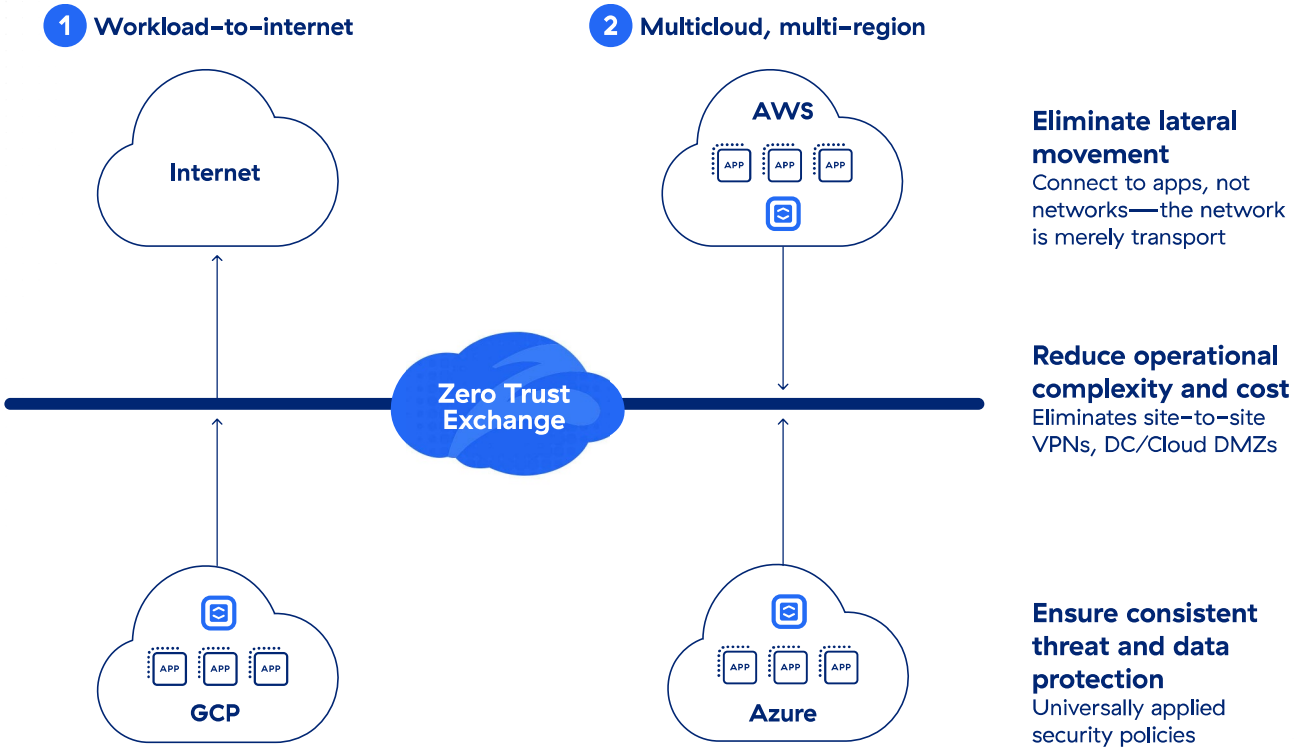
- Zscaler zero trust architecture ensures least privilege access for cloud workloads and applications. This means cloud workloads are connected only to authorized workloads, not to the corporate network using legacy network security architecture.

Reducing Operational Cost and Complexity

- Secure workloads across all major cloud service providers including AWS, Azure, and GCP using one unified platform.
- Automate security deployments through programmable interfaces using infrastructure as code (IaC) templates, along with Public Cloud Service Provider integrations such as AWS gateway load balancer, AWS user–defined tags, and AWS auto scaling

Gaining Consistent Threat and Data Protection

- Elevate cloud workload security to zero trust principles. Prevent zero-day attacks and protect data with cloud-scale TLS inspection, segmentation (across VPCs/VNets, regions, public clouds), advanced threat protection, and data loss prevention



Take advantage of Workload Communications

Zero trust security for workloads. Workloads benefit from zero trust security based on a multitude of contextual attributes, unlike traditional controls, which rely on networks or security.

Simplified business policy enforcement and management. 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.

End-to-end visibility with direct-to-cloud connectivity. Operators can gain full visibility of their egress traffic and control over how workloads communicate. Logging is centralized and streamed in real time, and logs can be exported to a SIEM or monitoring solution of your choice for correlation and analysis.

Hyper-scalability and performance, with no centralized chokepoints. The Zero Trust Exchange operates at hyperscale and can handle any increase in workload traffic with elastic, horizontal scaling. Zscaler's cloud native architecture also reduces network hops and associated latency to improve application performance.

High availability for reliable security. Workload Communications dramatically simplifies cloud configuration requirements because all the required services are transparently applied at scale in the Zero Trust Exchange.

Reduced costs with streamlined services delivered by the Zero Trust Exchange. With Workload Communications, there are no hidden costs—you're billed only for consumed security services.

Workload Communications use cases

Secure mission-critical cloud applications
Prevent zero day attacks, data loss, and ransomware attacks for mission-critical applications to ensure ongoing business operations.

Eliminate site-to-site VPN
Apply least-privileged access policies when connecting your cloud workloads located in different VPCs/VNets, regions, or public clouds with zero trust.

Accelerate Mergers and acquisitions integrations
Streamline post-M&A integration by enabling cross-network application access without connecting networks. Administer universal security posture to protect workloads across multiple VPCs, regions, and public clouds.

Secure cloud Virtual desktop infrastructure
Secure persistent and non-persistent VDI delivered from cloud infrastructure by applying policies to control access to explicitly allowed sites and private applications.

Workload Communications Capabilities

ZSCALER WORKLOAD COMMUNICATIONS PLATFORM	
FEATURE	**DETAILS**
Cloud Coverage	Supports securing workloads in AWS, Microsoft Azure, and Google Cloud Platform.
TLS/SSL inspection	Get unlimited TLS/SSL traffic inspection to identify threats and data loss hiding in encrypted traffic. Specify which web categories or apps to inspect based on privacy or regulatory requirements.
Log Streaming	Zscaler Nanolog Streaming Service consolidates logs from all workloads, globally, into a central repository that is determined by customers, where administrators can view and mine transaction data by cloud workloads in real time.
Infrastructure-as-Code	Zscaler provides terraform templates and providers that automate the provisioning and deployment of security policies and cloud connector virtual machines.

ZSCALER INTERNET ACCESS FOR WORKLOAD-TO-INTERNET	
FEATURE	**DETAILS**
Workload-to-Internet communication protection	Prevent cyber threats and data loss for workload-to-internet communications. Includes SSL inspection, IPS, URL filtering, and data protection for all communication.
URL filtering	Allow, block, caution, or isolate workload access to specified web categories or destinations to stop web-based threats and ensure compliance with organizational policies.
Advanced threat protection	Stop advanced cyberattacks like malware, ransomware, supply chain attacks, and more with proprietary advanced threat protection. Set granular policies based on your organization's risk tolerance.
Malware analysis	Detect, prevent, and quarantine unknown threats hiding in malicious payloads inline with advanced AI/ML to stop patient-zero attacks.
Intrusion prevention	Get complete threat protection from botnets, advanced threats, and zero-days, along with contextual information about the workloads . Cloud and web IPS works seamlessly across firewall, sandbox and DLP.
DNS security	Identify and route suspicious command-and-control connections to Zscaler threat detection engines for full content inspection.
DNS filtering	Control and block DNS requests against known and malicious destinations.
File control	Block or allow file download/upload to applications based on workload identity or application.
Bandwidth control	Enforce bandwidth policies and prioritize business-critical applications over recreational traffic.
Dynamic, risk-based access and security policy	Automatically adapt security and access policy to workloads, internet destinations, and content risk.
Correlated threat insights	Speed investigation and response times with contextualized and correlated alerts with insights into threat score, affected asset, severity, and more.

ZSCALER PRIVATE ACCESS FOR WORKLOAD-TO-WORKLOAD	
FEATURE	**DETAILS**
Workload-to-workload segmentation	Secure workload-to-workload connectivity and communication across hybrid and multicloud environments with ZPA for Workloads.
App discovery	Automatically discover and catalog applications using specific domain names and IP subnets to get granular insight into your private application estate, as well as your potential attack surface.
AI-powered app segmentation	Apply ML-based segmentation recommendations automatically delivered to you in ZPA, making it fast and easy to identify the right application segments and build the right access policies. Powered by ML models continually trained on millions of customer signals and your unique application access patterns, ML-based segmentation can help you minimize your internal attack surface.
AppProtection	Protect private applications and infrastructure against the most prevalent attacks with high-performance, inline security inspection of the entire application payload that exposes threats. Identify and block known web security risks, such as the OWASP Top 10, and emerging zero-day vulnerabilities that can bypass traditional network security controls.

DATA PROTECTION	
FEATURE	**DETAILS**
Inline data protection (data in motion)	For Workload-to-Internet and workload-to-workload, use forward proxy and SSL inspection capabilities to control the flow of sensitive information to risky web destinations and cloud applications in real time, stopping internal and external threats to data. Advanced inline protection is provided whether an application is sanctioned or unmanaged without requiring network device logs.
Exact Data Match (EDM)	Fingerprint and secure custom company data.
Index Document Match (IDM)	Fingerprint and secure custom documents and forms.
Optical Character Recognition (OCR)	Find and prevent data loss in images and screenshots.

(Capabilities listed are not collectively exhaustive. Specific features and capabilities may only be available with different Zscaler editions.)

Workload Communications unique value

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

- Application and 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, multitenant proxy architecture holds, inspects, and enforces policy
- High-performance inspection is done by a single-scan, multi-access architecture built for scale
- Fine-grained forwarding policy management for internet and non-internet traffic uses Zscaler Internet Access or Zscaler Private Access policies
- Unified, standardized policies across AWS, Azure, Google Cloud, and on-premises data centers include policy management, traffic monitoring, and log tracking

zscaler™ | Experience your world, secured.™

PRESIDIO®

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