zscaler™ 🟩 DATA SHEET

Zscaler Workload Communications

Secure workload-to-internet and workload-to-workload traffic for your cloud workloads with the power of the Zscaler Zero Trust Exchange™.

Digital transformation is driving the utilization of workloads across a wide array of on-premises, private cloud, and public cloud infrastructure environments. Your business runs on these workloads, so preventing cyberattacks and data loss is essential.

Legacy solution architectures are inadequate—they provide inconsistent threat and data protection, increase the attack surface, amplify lateral movement, and increase operational complexity and cost.

Zscaler Workload Communications radically simplifies hybrid workload security. With the power of the Zero Trust Exchange platform, it secures workload-to-internet and workload-to-workload egress traffic across public cloud and on-premises data centers for your mission-critical workloads and servers.

Workload Communications provides zero trust security that ensures consistent threat and data protection, eliminates the attack surface, stops lateral movement, reduces complexity, and lowers operational costs.

> “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

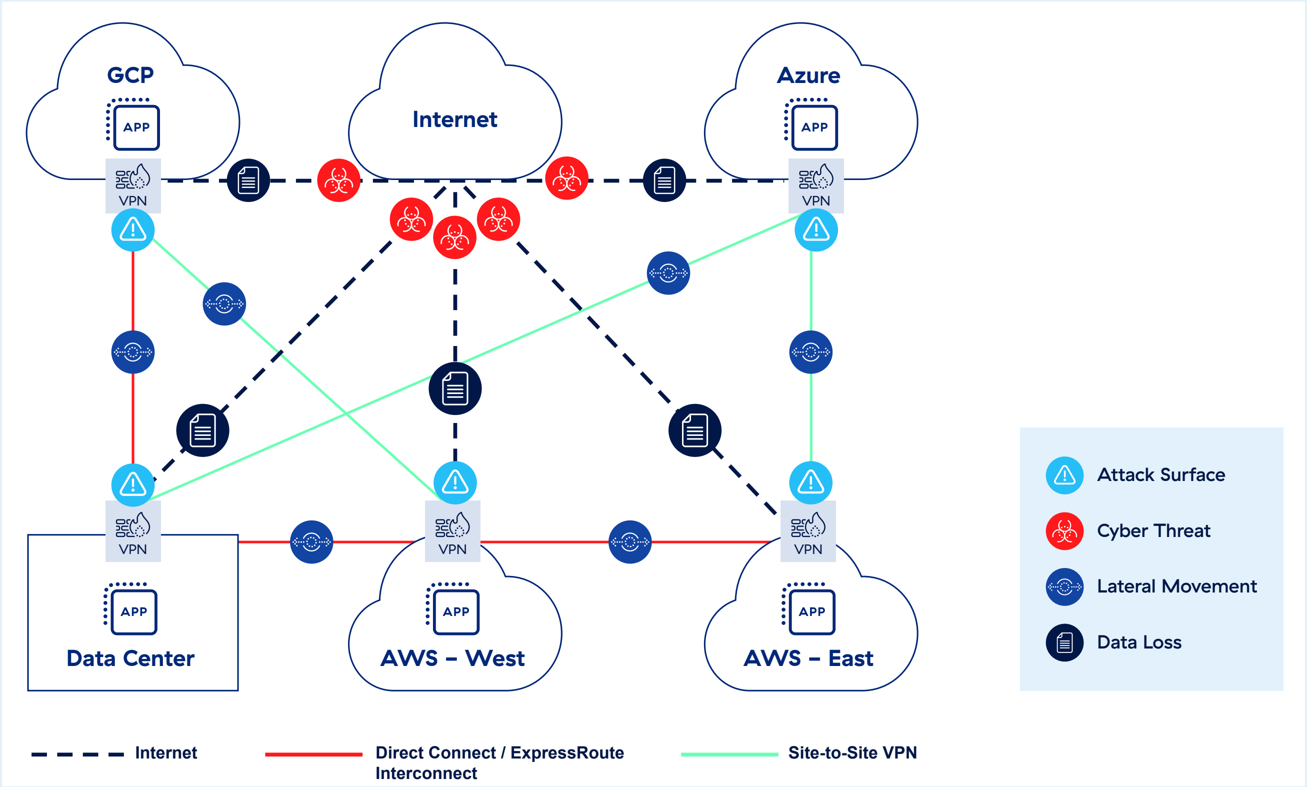
Challenges with legacy workload and server security

Many enterprises rely on legacy security architectures to secure their cloud workloads. Most use a combination of the following approaches:

- Configure native security solutions offered by public cloud service providers
- Deploy third–party tools (firewall, TLS/ SSL inspection, DLP, etc.) for extra layers of protection
- Backhaul traffic to on–premises network security infrastructure for inspection and protection

However, several challenges arise from this architecture, including:

- **TLS visibility gaps.** TLS inspection can use significant compute resources and 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 cybersecurity infrastructure costs to support scale.
- **Increased lateral movement and attack surface.** Solutions such as firewalls extend the network to workloads and servers, amplifying lateral movement risks. Each internet–facing firewall also 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 introduces both known and unknown gaps in security coverage, increasing security risk.
- **Increased complexity and poor performance.** Because legacy network and security solutions were not built with cloud workloads in mind, point products such as virtual firewalls, proxies, and NAT gateways must be incorporated. Some solutions may use separate VMs for each security function, resulting in sequential assembly line–style inspection, which increases latency. This creates significant operational complexities when applied across multicloud environments.
- **High costs.** Use of legacy network security point products (e.g., firewalls, IPS, routers), 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.
- **Lack of Common Logging.** Legal and regulatory mandates can require organizations to store logs for extended periods. Accessing these logs from different cloud environments and storing them in a central SIEM infrastructure can be complex and expensive.



Extend zero trust architecture to public clouds and on-premises data centers

Workload Communications eliminates the network attack surface by connecting workloads and servers to the internet and private applications with a zero trust architecture. This dramatically simplifies connectivity by reducing your organization's dependency on legacy solutions like firewalls while allowing for flexible forwarding and easing policy management with the proven policy framework of Zscaler Internet Access™ (ZIA) and Zscaler Private Access™ (ZPA).

This is all made possible by the Zero Trust Exchange platform, which operates at hyperscale and can handle any increase in workload or server traffic with elastic, horizontal scaling. With Workload Communications, all workload and server egress traffic is forwarded to the Zero Trust Exchange, where security policies can be applied for full TLS/SSL inspection and access control. Egress traffic is then forwarded to its intended destination, whether it's the internet, SaaS applications, or other workloads and servers hosted in other public clouds or data centers.

With Workload Communications, you can:

Gain Consistent, Comprehensive Threat and Data Protection

Enforce common security policies across all environments

- Prevent zero day-attacks with cloud-scale TLS inspection and threat protection
- Stop data leaks with DNS inspection and inline data protection
- Limit the destinations workloads and servers can access with strict controls

Eliminate the attack surface and lateral movement

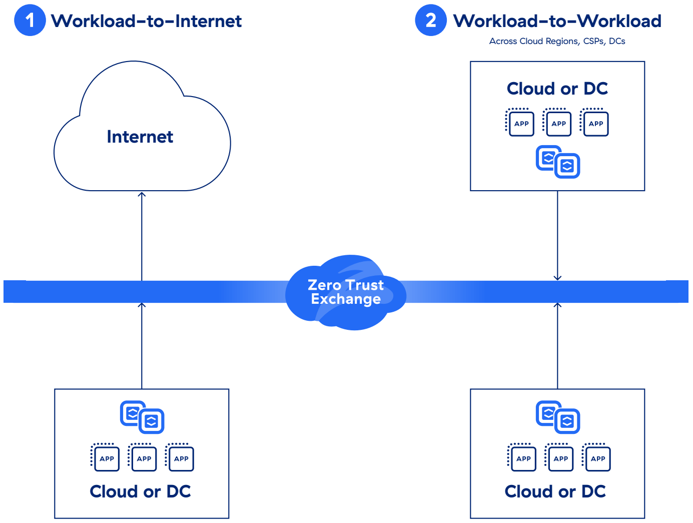
Connect apps not networks, become undiscoverable

- Apply least-privilege access to segment workloads using IP, FQDN, VPC, VNet, or Tags
- Connect workloads using the Zero Trust Exchange eliminating network attack surface
- Support cloud to cloud, cloud to data center, region to region

Reduce Operational Cost and Complexity

Use one cloud-delivered platform to secure all workloads

- 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
- Utilize Public Cloud Service Provider integrations such as AWS gateway load balancer, AWS user-defined tags, and AWS auto scaling



Consistent, comprehensive threat and data protection
Common security policies across all environments

Eliminates lateral movement and attack surface
Connect apps not networks, become undiscoverable

Reduces operational complexity and cost
One cloud-delivered platform to secure all workloads

Workload Communications Differentiators

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.

Zero Trust Proxy Architecture: Purpose-built, multitenant proxy architecture that sits inline to securely connect sources and destinations while providing full visibility of egress traffic.

TLS Decryption at Cloud Scale: High-performance inspection is done by a single-scan, multi-access architecture that is built for scale.

Bidirectional Threat Inspection: AI-powered threat protection—powered by 500 trillion daily signals and 320 billion daily transactions—delivers always-on, airtight ransomware protection, zero-day threat prevention, and unknown malware prevention.

In-line Data Protection: High-performance, scalable DLP inspection across all channels and locations.

Granular App-to-app Segmentation: Zero trust, least-privileged access for all workloads and servers provides simplified business policy enforcement and management.

Common Platform, Multi Cloud Ready: A unified platform provides policy management, traffic monitoring, and log tracking. Standardized policies are applied across AWS, Azure, GCP, and on-premises data centers.

Workload Communications Capabilities

ZSCALER WORKLOAD COMMUNICATIONS PLATFORM	
FEATURE	**DETAILS**
Public Cloud and On-premises Coverage	Supports securing workloads in AWS, Microsoft Azure, Google Cloud Platform, Microsoft Azure China regions and AWS GovCloud with additional support for on-premises data center servers. FedRamp Certified <> for AWS GovCloud.
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	Consolidate logs from all workloads and servers, globally, into a central repository determined by your organization, with Zscaler Nanolog Streaming Service. 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.
Connectivity Support	Leverage IPsec, GRE, or Cloud Connectors to steer workload egress traffic to the Zero Trust Exchange. (IPsec and GRE will secure workload-to-internet traffic. Cloud Connectors are used to secure both internet and workload traffic).

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 communications.
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, servers, 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.
Content filtering and stateful rules	Filter by policy across 6 classes, 101 categories, and 29 super-categories. Leverage dynamic content classification for unknown URLs and Safe Search. Apply granular policy by IP address, groups, and hosted identities.

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.
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)

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