Zero Trust Cloud

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

DATASHEET

Digital transformation is driving workload creation and utilization across a wide array of on-premises data centers, private and public clouds. Your business depends on these workloads, so preventing cyberattacks and data loss is essential.

Legacy architectures like firewalls and VPNs are inadequate—they provide inconsistent threat and data protection, increase the attack surface, leave the door open for lateral movement, and increase operational complexity and cost.

Zscaler Zero Trust Cloud radically simplifies hybrid workload security. With the power of the Zero Trust Exchange platform, it secures workload-to-internet and workload to-workload traffic across your on-premises data centers, private and public clouds.

Zero Trust Cloud provides consistent threat and data protection, eliminates the attack surface, stops lateral movement, reduces complexity, and lowers operational costs.

Challenges with legacy workload and server security

Many enterprises rely on legacy architectures to secure their cloud workloads. Most will do a combination of the following:

- Configure native security solutions offered by cloud service providers
- Deploy third-party tools such as firewall, TLS inspection, DLP, and more
- Backhaul traffic to on-premises network security infrastructure for inspection and protection

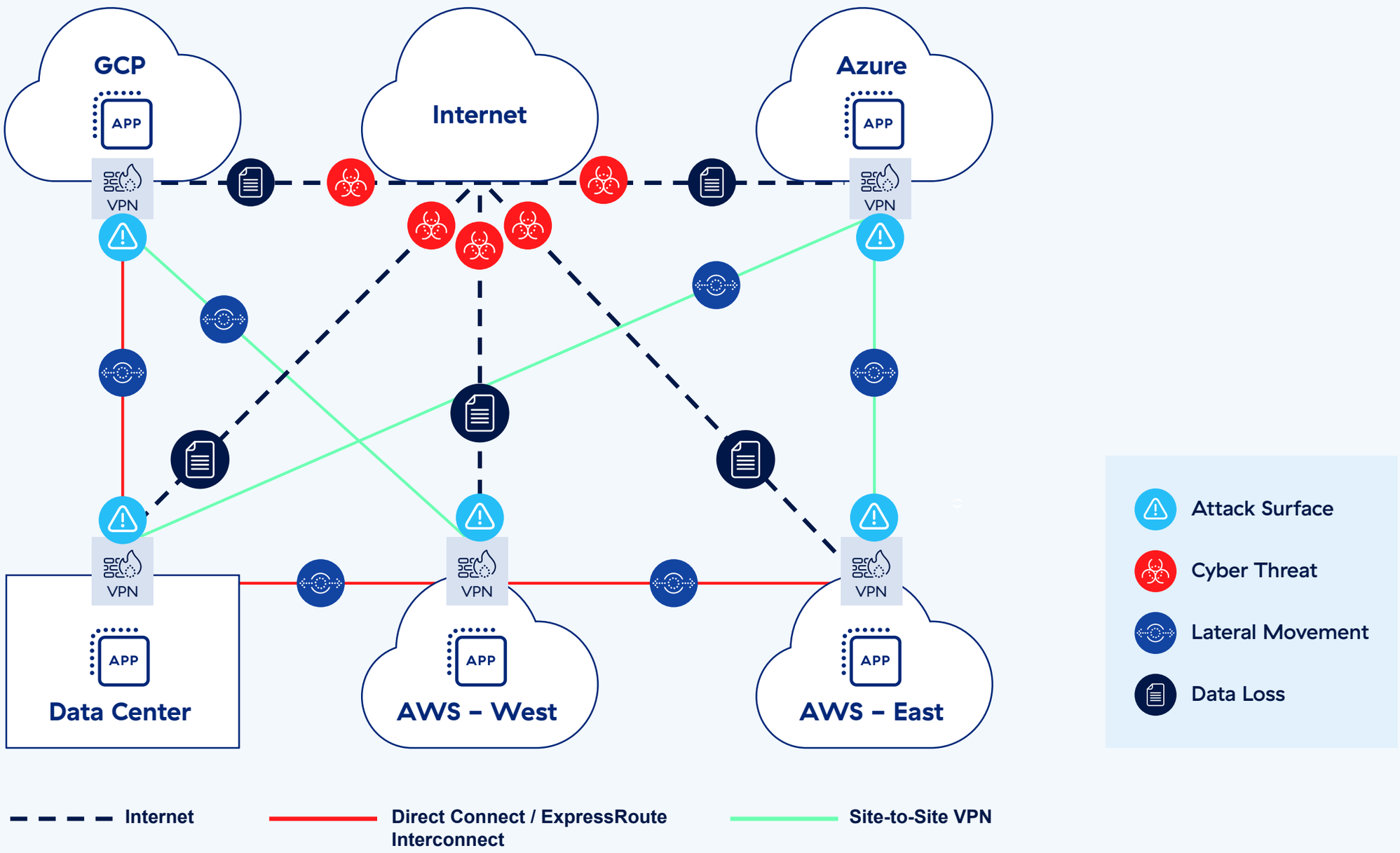
Using these methods introduces several challenges, including:

- **Increased attack surface and opportunity for lateral movement.** Solutions such as firewalls extend the network to workloads, amplifying lateral movement risk. 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.
- **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. TLS at scale increases operational and infrastructure costs.

- **Increased complexity and poor performance.** Legacy network and security solutions are not built with cloud workloads in mind, and so 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 such as firewalls and VPNs results in over provisioning of infrastructure. Implementing cloud native security tools across multiple CSPs requires highly specialized resources.

- **Inefficient log storage.** Some legal and regulatory mandates require organizations to store logs for extended periods. Accessing these logs from different cloud environments and storing them in a central SIEM can be complex and expensive.



Extend zero trust architecture to on-premises data centres, private and public clouds

Zero Trust Cloud eliminates the network attack surface by connecting your 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 and VPNs 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 that scales both vertically and horizontally. With Zero Trust Cloud, all workload 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, such as the internet, SaaS applications, or other workloads hosted in on-premises data centers, private or public clouds.

With Zero Trust Cloud, you can:

GAIN CONSISTENT, COMPREHENSIVE THREAT AND DATA PROTECTION

Enforce uniform security policies across all on-premises data centers, private and public clouds

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

ELIMINATE THE ATTACK SURFACE AND LATERAL MOVEMENT

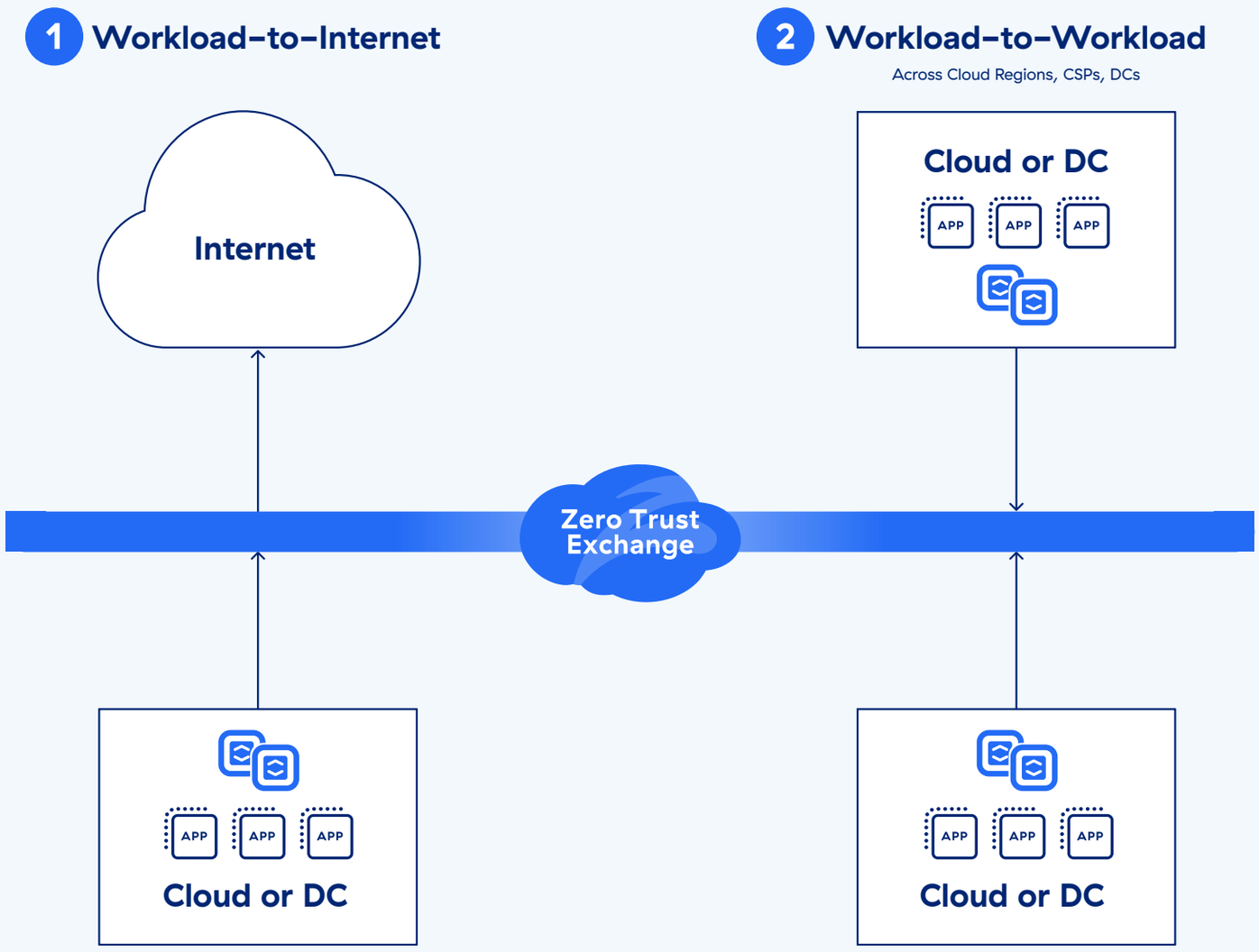
Connect apps, not networks—become undiscoverable

- Apply least-privileged access to segment workloads using IP, FQDN, VPC/Vnet,, or user defined tags
- Connect workloads using the Zero Trust Exchange, eliminating network attack surface
- Support cloud to cloud, cloud to data center, region to region, VPC/VNet to VPC/VNet and subnet to subnet

REDUCE OPERATIONAL COST AND COMPLEXITY

Use one security platform to protect all workloads in your clouds

- Secure workloads across major cloud service providers including AWS, Azure, and GCP using one unified platform
- Automate security deployments through programmable interfaces including Zscaler APIs, Hashicorp Terraform and AWS CloudFormation
- Leverage built-in integrations with CSPs to scale infrastructure, optimize cloud paths and simplify rule definitions with cloud metadata



Consistent 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

Zero Trust Cloud Capabilities

Zero Trust Cloud 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: Our 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.

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

Bidirectional threat inspection: AI-powered threat protection—powered by 500 trillion daily signals and 320 billion transactions processed each day deliver always-on, robust ransomware protection, zero-day threat prevention, and defense against unknown malware.

Inline data protection: High-performance, scalable DLP inspection across all channels and locations.

Common platform, Multicloud 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.

Zero Trust Cloud Features

ZSCALER ZERO TRUST CLOUD PLATFORM	
FEATURE	**DETIALS**
On-premises, Private and Public Clouds	Supports securing workloads in AWS, Microsoft Azure, Google Cloud Platform and on-premises data centers. It supports specialized regions including Microsoft Azure China and AWS China. Additionally it supports AWS GovCloud and Microsoft Azure GovCloud, with FedRAMP moderate and high certifications on both.
TLS/SSL Inspection	Get cloud-scale 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.
Intra-Region Segmentation	Secure workloads through segmentation across VPC to VPC or subnet to subnet within a specific cloud region. Support for source and destination tags in east-west traffic forwarding policy.
Log Streaming	Consolidate logs from workloads and servers, globally, into a central repository determined by your organization. Administrators can view and mine transaction data by cloud workloads.
Infrastructure-as-Code	Automate security deployments through programmable interfaces including Zscaler APIs, Hashicorp Terraform and AWS CloudFormation.
Connectivity Support	Use purpose built connectors or Zscaler managed service offerings to steer traffic. Optionally, leverage your existing IPsec or GRE tunnels.

ZSCALER INTERNET ACCESS FOR WORKLOAD-TO-INTERNET	
FEATURE	**DETIALS**
Workload-to-Internet Communication Protection	Prevent cyberthreats and data loss for workload-to-internet communications. Includes TLS 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 firewalls, sandboxing, 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	**DETIALS**
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. ML-based segmentation can help you minimize your internal attack surface with ML models continually trained on millions of customer signals and your unique application access patterns.
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	**DETIALS**
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 ZERO TRUST CLOUD EDITIONS	
FEATURE TIER	**CAPABILITIES**
Zero Trust for Workloads Standard	• Annual subscription by GB (Gigabyte) of monthly traffic for Zero Trust for Workloads Standard: • Includes Content Filtering
Zero Trust for Workloads Advanced	• Everything available in Workloads Standard edition • Internet Access for SSL/TLS inspection, Advanced Threat Protection, Cloud NSS, Source IP Anchoring • Private Access for Workloads: App Segments, Sub-Location, LSS Standard Logging and Reporting • Data Protection for Workloads: Inline web (in monitor mode only) • Cyber Protection for Workloads: Standard Firewall • East West Segmentation
Zero Trust for Workloads Advanced Plus	• Everything available in Workloads Advanced edition • Data Protection for Workloads: Data Protection inline and Advanced classification • Cyber Protection for Workloads: Firewall Advanced for Workloads, Sandbox Advanced for Workloads

Zero Trust Cloud is available in two deployment options. With the Virtual Machine (VM) option, customers get complete control of their cloud infrastructure by deploying the Zero Trust components as a virtual machine. With the Zero Trust Gateway, customers can consume the features as a cloud native service that is fully managed by Zscaler. Both deployment modes have feature parity with one another. Zero Trust Gateway is available in Zero Trust for Workloads Advanced and Zero Trust for Workloads Advanced Plus Editions.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**