EBOOK

How to achieve consistent security for workloads in multi-cloud

Contents

Introduction

Enterprises are migrating applications and workloads to the public cloud at an unprecedented pace, for all the right reasons.

Cloud transformation brings a rich array of benefits, ranging from cost savings to enhanced operational efficiencies and beyond. Making the move to the cloud is a key part of digital transformation, which enables an organization to become more agile; better meet the needs of customers, vendors, suppliers, and third-party partners; and boost customer experience.

As growing numbers of organizations across industries pursue cloud strategies in order to remain competitive with their peers, the public cloud has become the new enterprise data center. At the same time, hybrid and multicloud environments have become the norm. IDC Research recently predicted that by the end of 2025, a majority of enterprises will leverage the public cloud for generative AI platforms, developer tools, and infrastructure, with cloud usage surpassing that of on-premises systems.[1]

Top 3 cloud vendors hold 67% of market share

Gartner predicts that 51% of IT spending on application software, infrastructure, and organization process services will have shifted to the public cloud by 2025, overtaking spending on traditional IT.[4]

Even though cloud transformation has enormous momentum, with public cloud providers' combined revenues expected to exceed US$800 billion by the end of 2024,[2] the market is dominated by just three players:[3]

- Amazon Web Services (AWS), with 31% market share
- Microsoft Azure, with 25% market share
- Google Cloud, with 11% market share

These public cloud providers offer their customers new opportunities to tap into greater speed, agility, and elasticity when it comes to their use of computing resources. All make it possible for developers to spin up new environments in mere seconds. And all offer hundreds of different services—both self-managed and provider-managed.

However, these factors are also contributing to the emergence of new security risks, especially for organizations that continue to rely on legacy security architectures to secure their modern cloud environments. The fundamental mismatch—between traditional approaches to securing on-premises workloads and what's needed in today's cloud environments—often makes protecting cloud workloads costly, complex, and difficult.

1. IDC Research, IDC FutureScape: Worldwide Cloud 2024 Predictions, 2023.
2. IDC Research, Worldwide Semiannual Public Cloud Services Tracker.
3. Statista, Cloud Infrastructure Market, 2024.
4. Gartner, Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025.

Cloud workload security challenges

Organizations that migrate workloads to the cloud without modernizing their security approach in tandem face a host of common challenges.

Inconsistent or ineffective policy enforcement leaves workloads exposed to cyberthreats and attacks.

Relying on legacy approaches to secure and connect cloud workloads is inevitably complex and costly. Cybersecurity architectures based on firewalls and virtual private networks (VPNs) simply weren't designed for today's cloud computing ecosystems.

Exposed workloads can easily be compromised. Cybercriminals can hold organizations hostage with devastating ransomware attacks. Recovering from them can be costly and time consuming.

Cloud workloads require extensive communications with other workloads and the internet. Legacy security approaches are a poor match for this always-on connectivity.

44%

experienced a cloud-based data breach in 2024.[5]

49%

report that cloud complexity is a significant compliance and security challenge.[6]

69%

experienced budget overruns in their cloud spending in 2023.[7]

5. Thales Group, 2024 Cloud Security Study.
6. Ibid.
7. Gartner, 2024 Cloud Spending: IT Balances Costs with GenAI Innovation.

Today's applications are on the move. Zero trust should come along with them.

As remote and hybrid work has moved into the mainstream, organizations across industries are embracing zero trust to secure their users. In a zero trust approach, trust is never implicitly granted. Instead, it's assumed that every access request is hostile or compromised, and application access request is granted if and only if:

- Its identity and context (the "who, what, and where" of the request) can be verified
- The risks associated with that request can be evaluated in depth
- Policies can be enforced on a per-session basis

With growing numbers of applications and workloads moving to the cloud, it's essential that organizations extend the same degree of protection their users currently enjoy when it comes to application access to all their cloud assets and services. This means extending zero trust-based security to every one of your cloud workloads.

When organizations migrate their legacy monolithic applications to the cloud, they often choose to refactor them using a microservices approach. This makes it possible to take advantage of unique-to-the-cloud functionalities, such as specialized cloud databases, serverless functions, and event-driven architectures. This brings greater efficiency and can reduce costs, but it also creates a dynamic, highly automated environment. In this environment, communications are constantly being exchanged between workloads.

Cloud workloads must frequently:

- Connect to the internet
- Communicate with other workloads

The sheer number of communications that must be sent between workloads is much higher in this type of environment than it was in the legacy data center.

What is a workload?

A workload is the building block of a modern-day cloud application. In legacy on-premises environments, most workloads were components within large monolithic applications. That's not the case in today's cloud native environments, where applications typically consist of many modular components or microservices. Each service performs a specific task and communicates with other services to execute organization logic.

Examples of workloads include:

- Containers
- Virtual machines (VMs)
- Virtual desktop infrastructure (VDI) farms
- Serverless functions

Legacy network security doesn't work for the cloud native enterprise

Far too many organizations have embarked on their cloud transformation journey without changing their security strategy to keep pace. But legacy network security architectures were built for the on-premises data center, not the cloud. When organizations try to lift and shift them to the cloud, the resulting architecture is highly complex and ineffective.

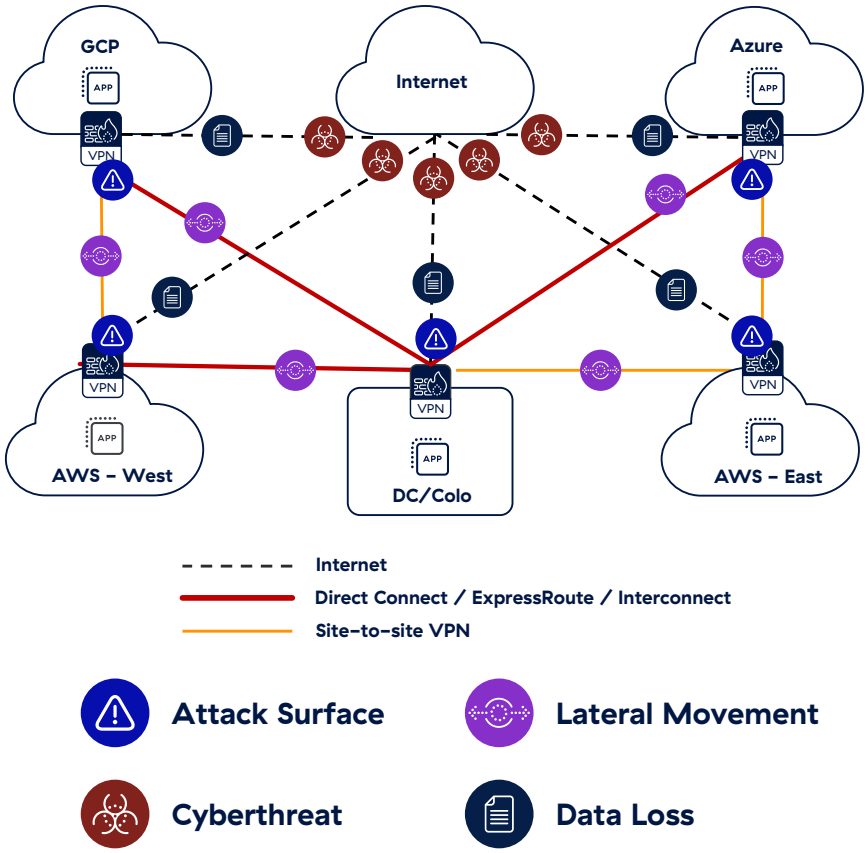
Cloud workloads must securely communicate with one another and with the internet. The legacy approach to achieving this involves building routable networks between cloud infrastructures by using firewalls and VPNs, essentially extending the organization wide area network (WAN) into the cloud.

In this model, organizations must stand up virtual next-generation firewalls (vNGFWs) everywhere their workloads reside. In a world where hybrid and multicloud environments are ubiquitous, this creates full mesh networks, in which each node connects directly to all the others. This architecture is enormously complex and challenging to manage.

If organizations want to implement additional security capabilities, such as data loss prevention (DLP) or TLS/SSL inspection, they'll need to layer on additional virtual security appliances, creating even more complexity.

Even within a single cloud service provider's environment, organizations will need to set up and manage multiple additional vNGFWs to secure north-south and east-west traffic between cloud workloads.

Workload communications multiply complexity and security challenges



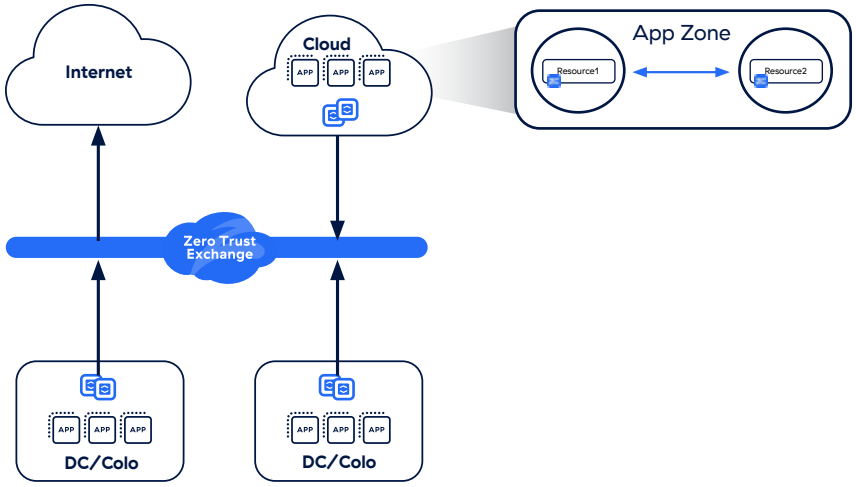
Inadequate cyber defense for today's computing ecosystems

Relying on legacy approaches to secure and connect cloud workloads leads to:

- **An expanded attack surface.** Each vNGFW has an identifiable network location and thus can be discovered by attackers. The more firewalls are deployed, the greater the attack surface.
- **Workload compromise.** Once bad actors discover an entry point into the environment and gain a foothold there, they're able to compromise workloads.
- **Lateral threat movement.** Because all workloads are connected via a mesh network, once a single workload is compromised, bad actors can move laterally across the network to compromise others.
- **No protection for sensitive data.** As they move across the network, attackers will be able to find and exfiltrate sensitive data such as customer financial information and trade secrets.

What's needed: a new approach to securing cloud workloads

Securing today's enterprise computing ecosystems, with their deep reliance on infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) from multiple cloud service providers and vendors, requires a different approach—one that puts the organization's security policies at the heart of its network design. This means enabling secure, least-privileged access based on direct workload-to-workload and workload-to-internet connectivity. Such an approach also makes it simple to build and maintain a zero trust architecture across all your cloud workloads.



With this new, modern approach:

- **The attack surface is eliminated.** Unlike with legacy solutions, workloads are effectively invisible to threat actors, essentially eliminating the entire attack surface.
- **Workloads are secured.** Full inline content inspection, along with DLP capabilities, delivers robust security for data and workloads.
- **Lateral threat movement is prevented.** Providing direct connectivity with no connection to a network renders lateral movement impossible.
- **Data is protected.** Adding TLS/SSL inspection at scale to DLP capabilities makes it possible to deliver comprehensive data protection at scale.
- **Complexity and cost are reduced.** Centralizing cloud configuration management along with security—and enabling direct connectivity—makes it possible to reduce complexity and costs.

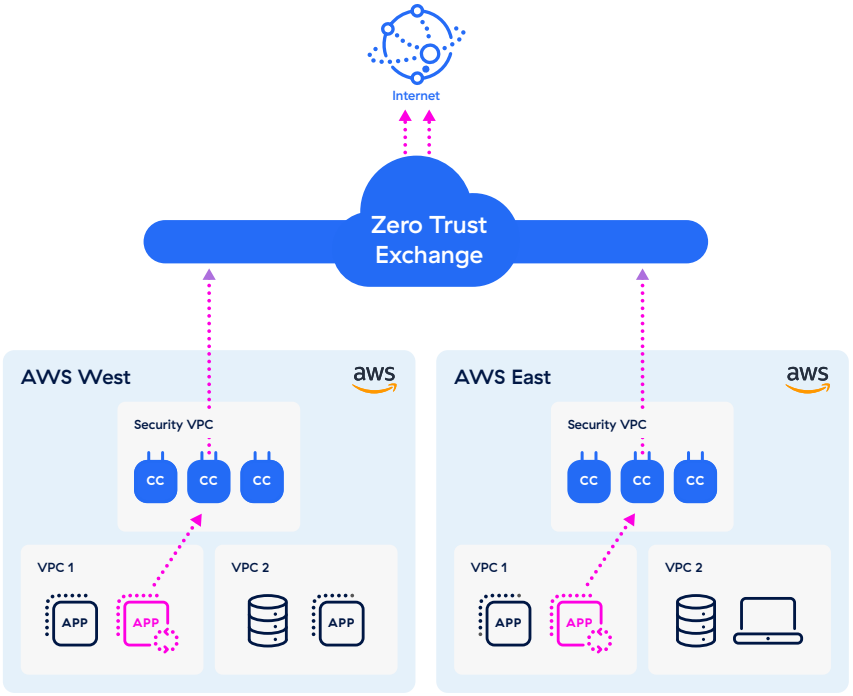
Simplify and secure workload-to-internet communications

Because every cloud workload relies on near-constant communication across the public internet, a zero trust solution for cloud workloads must be able to secure all outbound connectivity. Within a simple direct-to-cloud architecture, the solution must deliver secure internet access for all workloads, regardless of whether they're located in a public cloud or the enterprise data center.

Key capabilities needed to secure workload-to-internet communications include:

- Full proxy-based TLS/SSL inspection
- Zero attack surface
- Permitting access only to approved sites
- Advanced malware protection to block zero day threats

For example, let's imagine that your organization has apps located in AWS West and AWS East, and both require an update. The request will need to be forwarded to a central platform where policies are enforced and managed. An ideal solution will be able to enforce zero trust policies and connect sources and destinations securely.



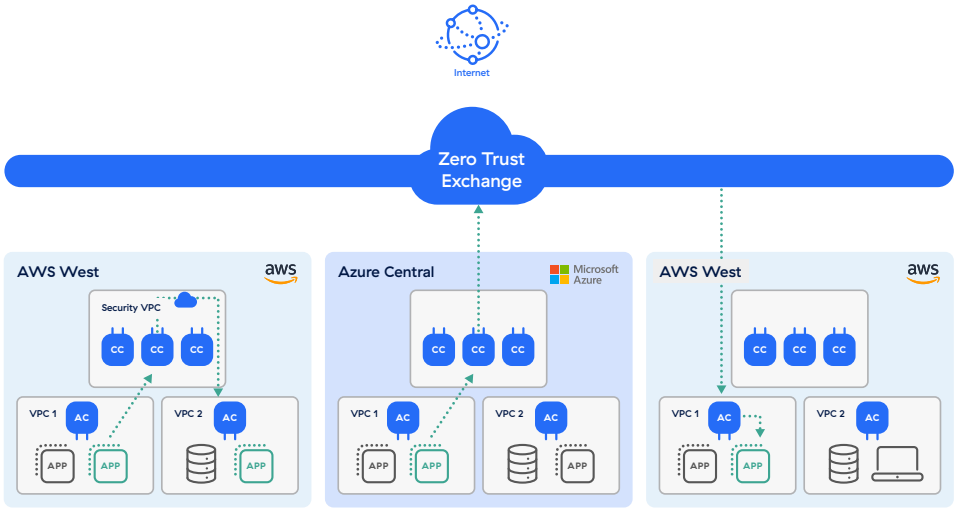
Simplify and secure workload-to-workload communications

Enforcing zero trust for cloud workloads also requires secure workload-to-workload connectivity. It's essential that workloads be able to communicate, both across multiple clouds and within a single virtual private cloud (VPC). These communications should flow through the central zero trust platform, where security policies are applied, and where identity and context are used to verify trust before permitting the connection.

In particular, there should be a mechanism to facilitate intra-workload communications. For VPC-to-VPC connectivity, traffic could be routed from one VPC to a private service edge, from which a connection would then be brokered to the destination app (located in a different VPC). For cloud-to-cloud connectivity, the traffic could be forwarded to a central zero trust platform, where a connection would be brokered to a destination app located in a different cloud.

Key capabilities needed to secure workload-to-workload communications include:

- Securing multicloud and multi-region connectivity
- Securing inter-VPC/inter-VNET connectivity
- Eliminating network attack surface with zero trust network access (ZTNA)
- Blocking lateral threat movement



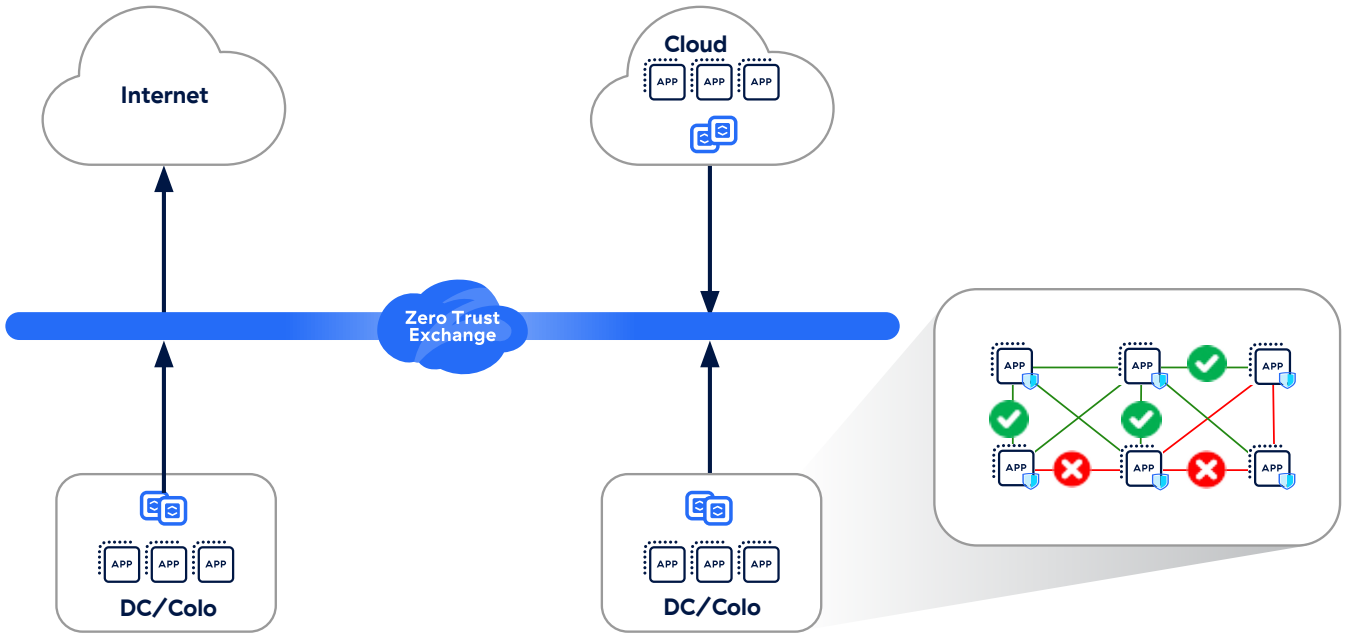
Easily achieve granular microsegmentation

A core component of zero trust security, microsegmentation prevents lateral threat movement by dividing groups of applications or workloads into small segments based on the communication requirements of individual applications. Workloads are permitted to communicate within their own segments, but cannot exchange unauthorized communications with workloads outside of them.

Microsegmentation makes it possible to enforce zero trust policies at a granular level throughout the organization's internal network, not just at its perimeter, extending consistent protections to on-premises workloads as well as those running in the cloud.

Key capabilities needed for workload microsegmentation include:

- AI-powered real-time resource discovery
- Host-based and non-host-based segmentation
- Ability to segment workloads within and across VPCs/VNETs



A zero trust solution for cloud workloads must have several key features:

#1: The ability to perform TLS/SSL inspection at scale

Many of today's most dangerous threats are hiding in plain sight in encrypted traffic. To detect them, you need a comprehensive platform that can perform complete TLS/SSL inspection at scale, without the performance limitations imposed by legacy applications.

Look for a solution that can offer:

- **Unlimited capacity** to inspect all your users' TLS/SSL traffic without performance concerns
- **Elastic scalability** based on traffic demands
- **Streamlined certificate management**
- **Granular policy control** that simplifies compliance by excluding encrypted user traffic for website categories like healthcare or banking

#2: Robust data protection capabilities

A defense-in-depth approach to data protection includes the ability to enforce data loss prevention (DLP) policies at scale without impacting performance. This provides an extra layer of protection. Should a cloud workload ever be compromised, there will still be a mechanism in place to enforce policies and prevent data exfiltration.

Look for a solution that can offer:

- **A streamlined dashboard** where DLP policies can be configured and managed
- **Advanced data management techniques** such as Exact Data Management (EDM) and Optical Character Recognition (OCR)
- **Reliable inline content inspection at scale**

#3: Advanced threat protection capabilities

To block today's most dangerous and sophisticated threats, a zero trust cloud workload security platform must be able to ensure that every packet, from every workload, can be fully inspected from start to finish. This requires integrated, always-on TLS/SSL inspection capabilities, as well as the ability to enforce fine-grained policies for all traffic.

In addition, key capabilities to look for include:

- **Integrated deception technologies** using decoys, lures, and honeypots to protect your most valuable assets with high fidelity and low false positive rates
- **Cloud sandboxing** to quarantine and inspect potential threats rather than allowing them to pass
- **Malware protection** that can block known ransomware, spyware, and malware, as well as novel threats

#4: Comprehensive host-based segmentation

Microsegmentation prevents lateral threat movement to minimize the blast radius and damage that a cyber incident might cause. Host-based microsegmentation relies on agents installed on endpoint devices to provide control and visibility that's much more granular, making it easier to manage identity-based segmentation. Using an agent enables segmentation based on dynamic, human-understandable policies rather than static network-level rules.

In particular, look for a solution that can provide:

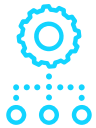
- **Real-time resource discovery** leveraging AI to give you granular visibility across all devices, services, and assets within your enterprise ecosystem
- **Zero trust policy recommendations** based on traffic analysis
- **Integration with a zero trust platform,** so that you can protect and segment your environment in just one place, with no need to deploy multiple point products

The top use cases for securing workload connectivity

A zero trust–based solution for workload connectivity can help organizations solve several key challenges. Here are four of the most common:

Securing traffic to the internet

When applications communicate with the internet or SaaS applications, the egress traffic needs to be inspected for cyberattacks and data leaks. Zscaler operates the world's largest inline cloud security platform, which delivers advanced threat protection at cloud scale without any performance impact or service degradation.



Workload segmentation

With the right workload communications solution, it's possible to take a granular and methodical approach to workload segmentation. This makes it simpler to apply policies to control connectivity for workloads across VPCs, regions, and public and private clouds.

Cloud migration

This is often a time–consuming and arduous process for organizations. They must consider many factors, including which migration strategy to follow. Does it make sense to do a simple life and shift, or should apps be refactored or rebuilt? The right workload communications solution can make it simpler and easier to connect newly migrated cloud apps securely.

Mergers and acquisitions (M&A)

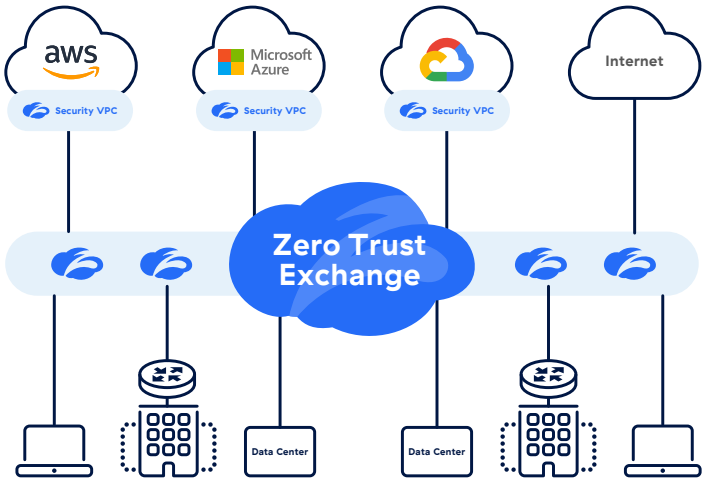
With a modern, zero trust–based, cloud native workload communications solution, it's possible to provide secure cross–network application access, with no need to redesign and rearchitect networks to connect them.

Zscaler Workload Communications is the answer

Looking for an end-to-end solution that can do all this and more? The Zscaler Zero Trust Exchange™ has made it possible to completely reimagine workload communications within a simple, proven, direct-to-cloud architecture.

Combining Zscaler Internet Access™ (ZIA) for workload-to-internet communications, Zscaler Private Access™ (ZPA) for workload-to-workload communications, and segment-of-one zero trust microsegmentation capabilities, Zscaler Workload Communications is a comprehensive approach to securing cloud and on-premises workload connectivity. At the same time, it's able to maintain performance to ensure your users have great experiences, and scalability to keep pace with the evolution of your cloud footprint as your operations grow.

Zscaler Workload Communications provides highly effective zero trust-based cloud security that can scale along with your needs. Elastic autoscaling capabilities enable it to handle traffic increases with ease. The Zero Trust Exchange already operates at hyperscale, with more than 150 data centers around the globe. Zscaler handles all updates automatically on your behalf, and the infrastructure is natively integrated with public cloud providers' security infrastructure, leveraging functionalities like transit gateways and load balancers.



In addition, Zscaler Workload Communications simplifies and centralizes policy management. All policies can be created and updated in a single, central, easy-to-use console. They're applied within the Zero Trust Exchange, where either ZIA or ZPA policies can be leveraged to provide full content inspection and identity-based control of workload communications. From there, the communications can be forwarded to any destination, whether that's the internet or other private applications within cloud environments. Policies can be readily applied at scale whenever you need to deploy additional workloads in the cloud.

If you're interested in learning more about the benefits of using Zscaler Workload Communications, contact us today. You can also learn more by visiting the Zscaler Zero Trust Cloud Connectivity webpage.

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 SASE–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