Zscaler on Zscaler

Securing Cloud Environments and Workloads with Zscaler Zero Trust Cloud

WHITEPAPER

Introduction

As more organizations embrace the cloud to drive digital transformation, the complexity of securing workloads across diverse environments has grown exponentially. We put Zscaler to work inside Zscaler, securing internal users, workloads, and environments while helping customers do the same. Our “Zscaler on Zscaler” initiative allows us to realize the full potential of a cloud-native Zero Trust architecture for securing egress workload traffic, connecting workloads securely across clouds, and maintaining visibility into sensitive data and misconfigurations through proactive monitoring.

Through our integrated approach, we eliminate the risks of traditional security models, reduce attack surfaces, and provide a strong foundation for safe and scalable cloud operations.

Why Cloud Security is More Critical Than Ever

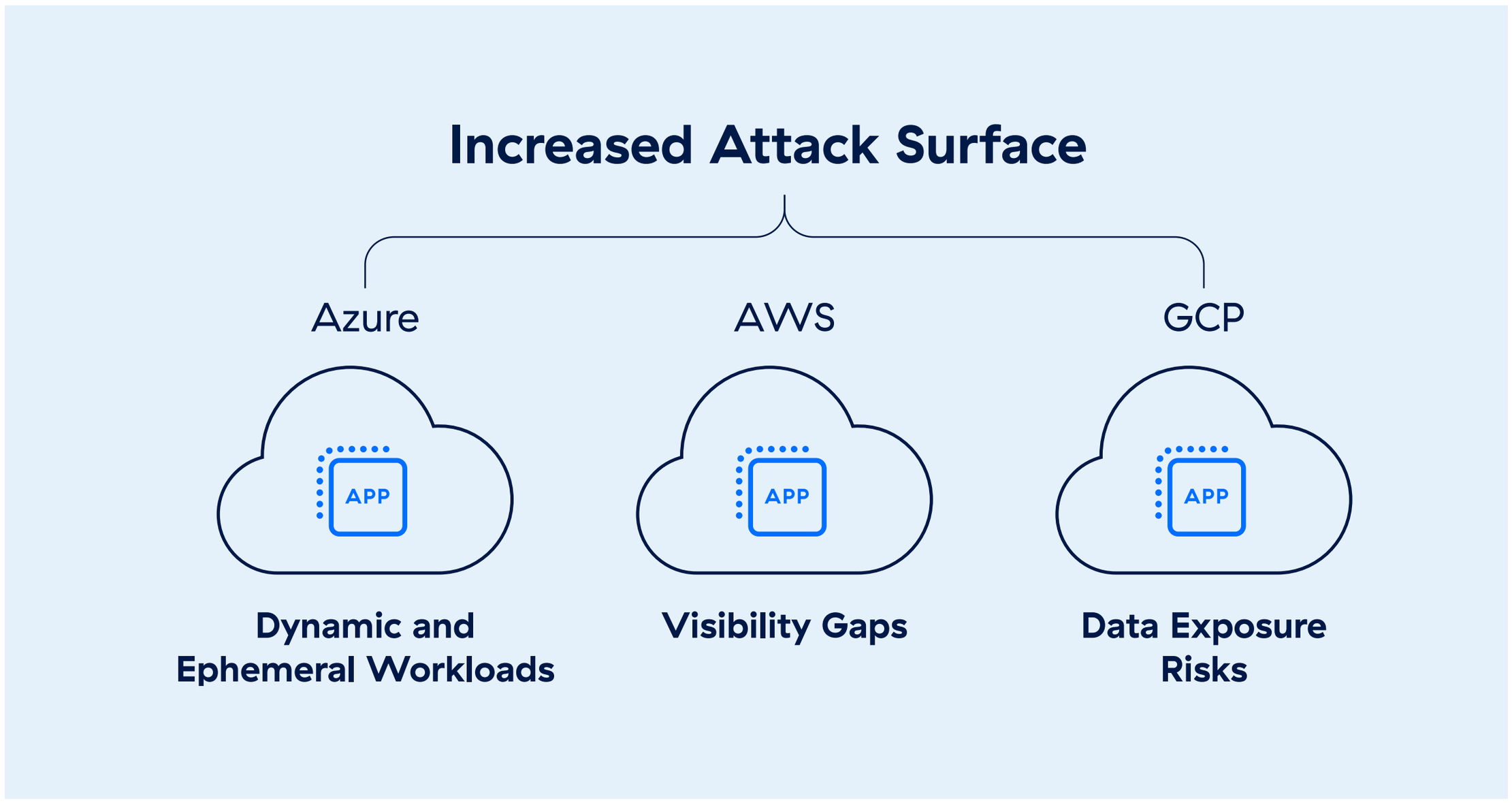
The shift to public and multi-cloud environments provides businesses with unparalleled flexibility and scalability. However, this transition also introduces new risks, including:

- **Increased Attack Surface:** Dispersed workloads spread across multiple clouds, regions, and networks create new vulnerabilities. Traditional perimeter-based security models are no longer adequate as traffic moves east-west within clouds and across environments.

- **Data Exposure Risks:** With sensitive data flowing between workloads and cloud environments, misconfigurations or a failure to enforce data governance policies can lead to breaches or regulatory non-compliance.

- **Dynamic and Ephemeral Workloads:** Containers, serverless functions, and software-defined networking enable speed and agility but add complexity, making it difficult to enforce consistent security policies at scale.

- **Gaps in Visibility:** The ephemeral and distributed nature of modern workloads can lead to visibility gaps, making it challenging to identify misconfigurations, vulnerabilities, and anomalous behavior.

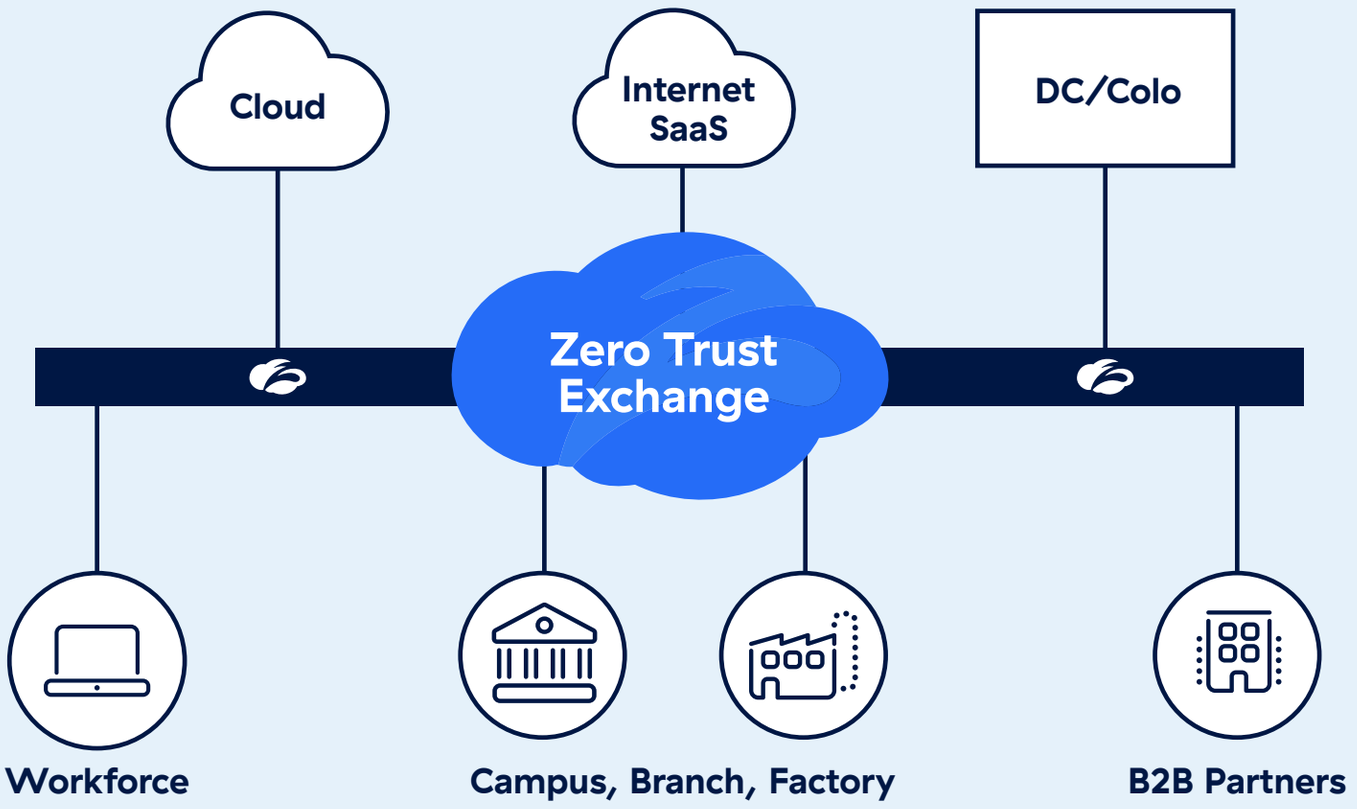


Challenges of Managing Cloud Security at Scale

- **Hybrid and Multi-Cloud Interoperability:** Securing workloads that span multiple cloud providers (AWS, Azure, GCP) and hybrid-cloud setups demands consistent policies and integrations.
- **Inefficient Traditional Architectures:** Relying on VPNs, firewalls, and other legacy security technologies often results in complex configurations, poor scalability, and performance bottlenecks.
- **Lateral Movement Risk:** Many organizations still operate in a "trust but verify" framework, leaving them vulnerable to insider threats and lateral movement of attackers.
- **Data and Configuration Mismanagement:** The lack of comprehensive solutions for detecting sensitive information in real time or identifying cloud misconfigurations can lead to non-compliance and breaches.
- **Operational Complexity:** Scaling security controls and ensuring seamless connectivity across distributed teams, environments, and applications introduces engineering challenges that strain IT teams.

Zscaler's Approach to Securing Our Own Cloud Environments

At Zscaler, we designed a robust, scalable solution for securing cloud environments and workloads at the enterprise level. Zscaler was not immune to many of the common cloud challenges while we were growing and maturing as a global multi-cloud enterprise. We needed to slow down and take control of the exponential growth of our cloud environments. We deployed our own products and addressed the common challenges outlined above.



Technical and Strategic Foundations

Securing Workload-to-Internet traffic:

- Zscaler Cloud Connectors allow workloads in VPCs/VNETs to connect to the internet securely, with direct-to-cloud connectivity and security inspection.
- Eliminate the need for firewalls, reducing complexity and having a consistent, centrally managed security policy across multi-cloud environments.
- Eliminating the need for VPNs and backhauling, Cloud Connectors enable seamless, secure, and scalable connectivity without introducing latency.
- Security capabilities encompass URL and Cloud Application filtering, DNS security, Advanced Firewalling, and comprehensive flow visibility and logging.

Connecting Workload-to-Workload Communication:

- ZPA creates secure, zero trust connections between workloads hosted in cloud agnostic environments or regions without cumbersome routing, VPN's and public exposure.
- Workload-to-workload communication bypasses the public internet entirely, drastically reducing the attack surface and preventing unauthorized lateral movement.
- By integrating application segmentation into the architecture, resources remain invisible to external entities unless explicitly authenticated and validated for their posture. This approach also delivers comprehensive logging and visibility, eliminating the need for separate third-party tools or independent cloud configurations.

Cloud Security Posture and Data Security Posture Management:

We leverage a comprehensive approach to maintaining cloud security posture, ensuring continuous monitoring against misconfigurations and policy violations within our cloud environments. By aligning tightly with key regulatory frameworks (e.g., ISO, NIST, HIPAA, GDPR).

We prioritize compliance and proactive risk management. Our workflows are designed to mitigate risks, address cloud misconfigurations efficiently, and reduce the potential for human error or cloud drift.

Our DSPM capabilities focus on identifying, classifying, and protecting sensitive data distributed across our cloud environments. With robust data governance practices, we maintain control over sensitive information while minimizing the risk of exposure.

Leveraging advanced tools for automated risk assessment, we quickly identify and address potential threats, ensuring consistent data security and reducing the impact of emerging risks.

Transformational Journey

Zscaler's commitment to innovation and adaptability in a cloud-first world is exemplified by our journey of securing cloud environments with our own products. Utilizing solutions like Zero Trust Cloud, Workload-to-Internet and Workload-to-Workload, we have successfully transformed our security infrastructure to be simpler, more efficient, and grounded in zero trust principles. This approach not only fortifies Zscaler's internal operations but also highlights the power of our solutions on a global scale.

Securing the cloud is an ongoing process at Zscaler, demanding continuous refinement of defenses to combat evolving threats. This iterative approach leverages real-world threat intelligence and internal insights, fostering a feedback loop with product teams. This collaboration not only strengthens Zscaler's internal security but also drives product innovation, ensuring both Zscaler and its customers remain ahead of attackers.

Ultimately, Zscaler's own experience demonstrates that cloud security is a continuous transformation, not a one-time effort. By consistently adapting to the dynamic threat landscape, Zscaler maintains its leadership in cybersecurity, protecting itself and empowering organizations globally.

Looking ahead, we are focused on increasing automation and self-service capabilities to further empower our teams. By enabling workflows where developers can seamlessly request cloud environments, we aim to embed security directly into development pipelines from the start. These workflows will automate approvals, stand up complete cloud environments, and apply vital networking and security constructs—like App Connectors, Cloud Connectors, and zero trust settings—before a single connection is made. This approach ensures consistency and security while accelerating innovation and product delivery, allowing Zscaler to remain at the forefront of secure, scalable technology.

Operational, Security, and Business Benefits

Operational Benefits:

- Simplifies deployment & management
- Unified policy enforcement across cloud/regions
- Cloud-native scalability

Security Benefits:

- Reduced attack surface with Zero Trust
- Real-time visibility & proactive mitigation
- Centralized data-flow & vulnerability insights
- Secure East-West communication

Business Benefits:

- Cost reduction
- Stronger compliance posture
- Accelerated innovation

Operational Benefits:

Our cloud-native Zero Trust approach improves efficiency by simplifying deployment and day-to-day management, increasing operational agility while freeing IT teams to focus on higher-value work. Using standardized Terraform-based automation, we rapidly deploy Cloud Connectors and App Connectors to speed time-to-value and ensure repeatable, consistent implementations. Building on this foundation, Zscaler on Zscaler is developing a self-service catalog through our ITSM platform that enables teams to request complete cloud environments delivered end-to-end through automated workflows—including provisioning core cloud constructs such as VPCs/VNETs, IAM roles, and baseline networking, as well as deploying Cloud Connectors and App Connectors to establish security and connectivity from the start. What previously required weeks of manual effort is being transformed into pipelines that complete in minutes. In parallel, centralized policy enforcement ensures consistent governance across all workloads, regions, and cloud providers. Finally, our architecture scales seamlessly as the business grows, without requiring disruptive infrastructure redesigns or operational rework.

Security Benefits:

Zero Trust Cloud significantly reduced our attack surface by eliminating implicit trust, which blocks lateral movement and mitigates both insider and external threats. This approach provides enhanced visibility and proactive mitigation through real-time monitoring. It offers complete oversight of sensitive data and vulnerabilities, enabling teams to respond quickly to issues. This visibility was achieved without relying on third-party logging solutions or encountering difficulties in extracting logs from cloud platforms. Insights into data flows, both internal and external, were immediately accessible within the central logging systems of ZIA and ZPA.

Moreover, our cloud solution ensures secure East-West communication. By routing East-West traffic through ZPA, sensitive workloads are isolated from opportunistic and targeted attacks, even during inter-cloud communications, bolstering overall security.

Business Benefits:

One key benefit is significant cost reduction, achieved by eliminating the need for outdated security appliances, cloud firewalls, VPNs, and the associated manual oversight, thereby lowering operational expenses.

Another advantage is strengthened compliance, as continuous monitoring ensures adherence to regulations. This mitigates audit concerns and potential penalties.

Finally, by using our own products it unlocked accelerated business innovation. By offering a secure-by-design infrastructure, teams can build, deploy, and scale new applications without security impediments.

BY THE NUMBERS

1000
Cloud connectors deployed in AWS, GCP & Azure

650
GB per month of workload traffic secured

15.5
Billion sessions monthly

Conclusion

The dynamic, distributed nature of modern cloud environments requires a fundamental shift from legacy security models to a zero trust architecture. By adopting our own Zscaler solutions, we have built a foundation for secure, scalable operations that mitigate risk, protect sensitive data, and enable seamless workload connectivity across regions and cloud providers.

Zscaler's Zero Trust Cloud — including Cloud Connectors, ZPA, DSPM, and CSPM — enables us to tackle cloud security challenges while reaping significant operational and business benefits. Through this approach, we ensure that our cloud environments remain robust and flexible — an invaluable use case for delivering on the promise of secure digital transformation for organizations worldwide.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform 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 in-line 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**

zscaler™

Act Fast.
Stay Secure.