Zscaler™ Cloud Protection at a Glance

Zscaler Cloud Protection (ZCP) Benefits:

Secure cloud security posture

Continuous inventory and remediation of all services in cloud platforms (Azure, AWS, GCP) and SaaS apps

Secure user access to cloud workloads

Zero trust provides user access with no exposed attack surface and no VPNs

Secure app-to-app communication

Secures and simplifies workload communications to the internet, data centers, and across clouds

Elimination of lateral threat movement

App identity and ML automation simplify microsegmentation and stop east-west propagation of threats

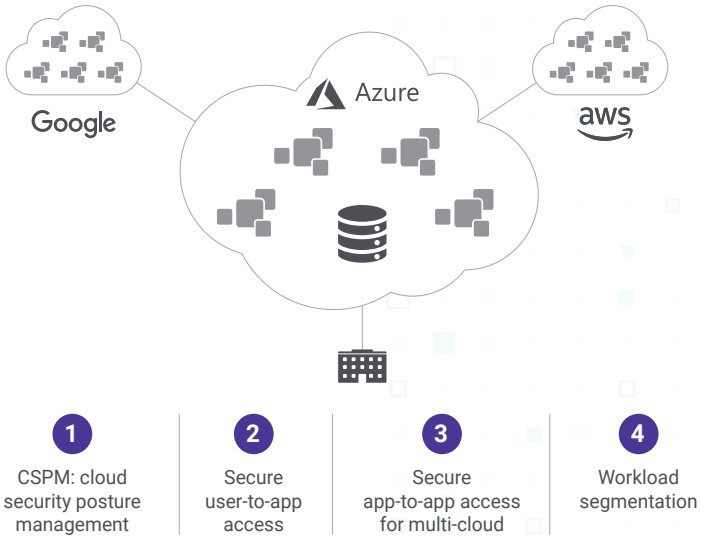
Cloud continues to accelerate digital transformation in every industry, ushering in a new era of scale, performance, and agility for enterprise cloud applications. Unfortunately, the same cloud attributes that allow enterprises to move fast and scale have resulted in security exposures and breaches.

The "lift-and-shift" approach of adapting legacy data center security to public cloud environments is costly, complicated, and static, making it impossible for InfoSec teams to keep pace with the speed of DevOps development and deployment.

ZCP builds on the Zscaler Zero Trust Exchange architecture to reduce the risk of moving to the cloud while reducing operational complexity. The four elements of ZCP address the key security and operations challenges that must be overcome for secure cloud deployment:

- Identifying workloads in the cloud and ensuring they have a strong security posture
- Ensuring safe application access for authorized users only
- Allowing workloads to securely access other clouds, data centers, and the internet as needed
- Mitigating risk by restricting an attacker's lateral movement

The four elements of ZCP



Zscaler Cloud Protection Key Capabilities

Cloud security posture management

- Inventory, continuously monitor, and automatically remediate all cloud services, including IaaS, PaaS, containers, serverless, and more
- Deep policy coverage across AWS, Azure, GCP, and SaaS with 3,000+ pre-built policy templates and mapping to 16 major regulatory frameworks

Secure user-to-app access

- Leverage zero trust to provide access to applications, not to your network, limiting potential threats from the outside without any of the management headaches, poor user experiences, or exposed attack surfaces that occur with traditional VPNs

Secure app-to-app communication across clouds

- Automatically deploy and configure cloud-to-cloud and cloud-to-DC connectivity without the complexity, overhead, and cost of managing transit gateways, transit hubs, virtual firewalls, VPNs, routers, networking policies, and peering
- Secure and simplify cloud-to-internet access with the proven scalability, performance, and reliability of the Zero Trust Exchange to ensure safe, controlled access from any cloud with no exposed attack surface

Identity-based microsegmentation

- Verify the identity of cloud and DC workloads and automatically microsegment any cloud or DC to eliminate the attack surface and stop lateral movement and the propagation of malware
- Reduce policies by 90 percent or more

"Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement, and mistakes."

– Gartner

To learn more about what Zscaler Cloud Protection can do for you, go to **zscaler.com/ZCP** ›

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com