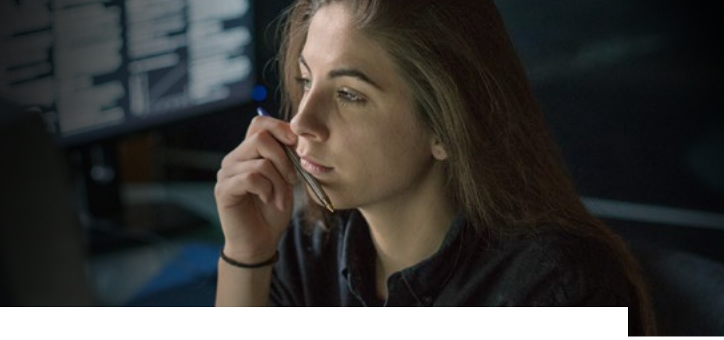
zscaler™

Zscaler Workload Posture: At-a-Glance



Zscaler Workload Posture Benefits:

Cloud Configuration and Compliance Assurance

Benchmark public cloud configurations against best practice standards and compliance frameworks to report misconfigurations, policy violations and automate remediation.

Privileged Identities Governance

Detect and remediate excessive or unused cloud permissions and enforce the least privilege without disrupting productivity.

Data Protection

Identify and protect sensitive or exposed data inside SaaS applications and IaaS offerings, such as AWS S3 with Integrated data loss prevention.

The Challenge

Moving applications to the cloud has allowed organizations to rapidly respond to changing customer needs, be more agile to changing business requirements, and save money.

Along with the significant benefits, the shift to the cloud has also amplified the threat landscape. The benefits of agility and efficiency come with the challenge of securing assets and workloads in the cloud. The rapid adoption of public clouds like AWS, Azure, GCP, and an increasing number of cloud services, has created an explosion of data and identity complexity with unmanaged risk. Security, access, and compliance management remain the most significant barriers to successful cloud adoption.

Traditional network-based security perimeter concepts, even when virtualized, do not solve the challenges unique to the cloud and hybrid deployments, add unnecessary cost, and are too complex to deploy, negating the cloud's very agility and scalability benefits.

Zscaler Workload Posture automatically identifies and remediates cloud service, application, and identity misconfigurations in SaaS, IaaS, and PaaS to reduce risk and ensure compliance. Workload Posture is part of Zscaler Cloud Protection, a comprehensive multi-cloud security platform covering misconfigurations, entitlements, exposed attack surfaces, lateral threat movement, and data loss.

Key Highlights

- Multi-cloud asset, entitlement, and compliance visibility
- AWS, Azure, and Google Cloud coverage
- Identify misconfigurations, identity, and access risks, sensitive data classification, and protection
- Risk-based prioritization of security and identity issues
- Auto remediation with DevOps integrations
- Enforce best practices and least privileged practice

Gartner has reported that 99% of cloud security failures will be the customer's fault over the next three years, and 75% of these failures will result from improper management of identities, access, and privileges.

Zscaler Workload Posture Key Capabilities

→ Discover Assets

Gain 360-degree visibility and discover all assets, identities, crucial databases, entitlements, and configurations along with their activities, relationship, and associated security risk in a single interface with rich analytics.

→ Identify and Prioritize Risk

Identify, prioritize, and fix the most critical security and IAM risk with Risk-based prioritization.

→ Remediate Risk

Leverage step-by-step guided or auto-remediation to mitigate identified misconfiguration and policy violations. Enforce least privileges, automate privilege right-sizing, and eliminating excess privileges.

→ Compliance Assurance

Automatically validate all configurations against pre-built mapped 2700+ industry best practices and 16+ compliance frameworks such as GDPR, PCI, NIST, CIS, and the custom framework.

→ DevSecOps

Integrate and enforce security, compliance checks at the development stage to keep up with DevOps deployment speed.

→ Secure K8S Configurations

Identify Kubernetes misconfigurations, processes running as root, privileged containers, compliance violations, and secure various Kubernetes deployments like AKS and EKS.

→ Integration

Easily integrate with current SecOps ecosystems such as ServiceNow, Zendesk, or Splunk so that the SecOps team can act immediately and effectively.

→ Easy Implementation

ZWP, a multi-tenant SaaS API-based solution, gets deployed in minutes with read-only access permission at scale without limitation and complexities.

→ Security Enforcement

Quickly implement unified guardrail policies to prevent misconfigurations and enforce the least privileges with the pre-built best cloud security policies and ML-based model without disrupting productivity.

→ Automated Data Classification and Protection

Zscaler data protection automatically identifies sensitive information in the cloud to secure SaaS like Microsoft 365 and IaaS offerings like AWS S3.

> "Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement, and mistakes."
>
> **– Neil MacDonald, Analyst, Gartner**
> Innovation Insight for Cloud Security Posture Management

To learn more about what Zscaler Workload Posture can do for you, go to **zscaler.com/products/workload-posture ›**

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