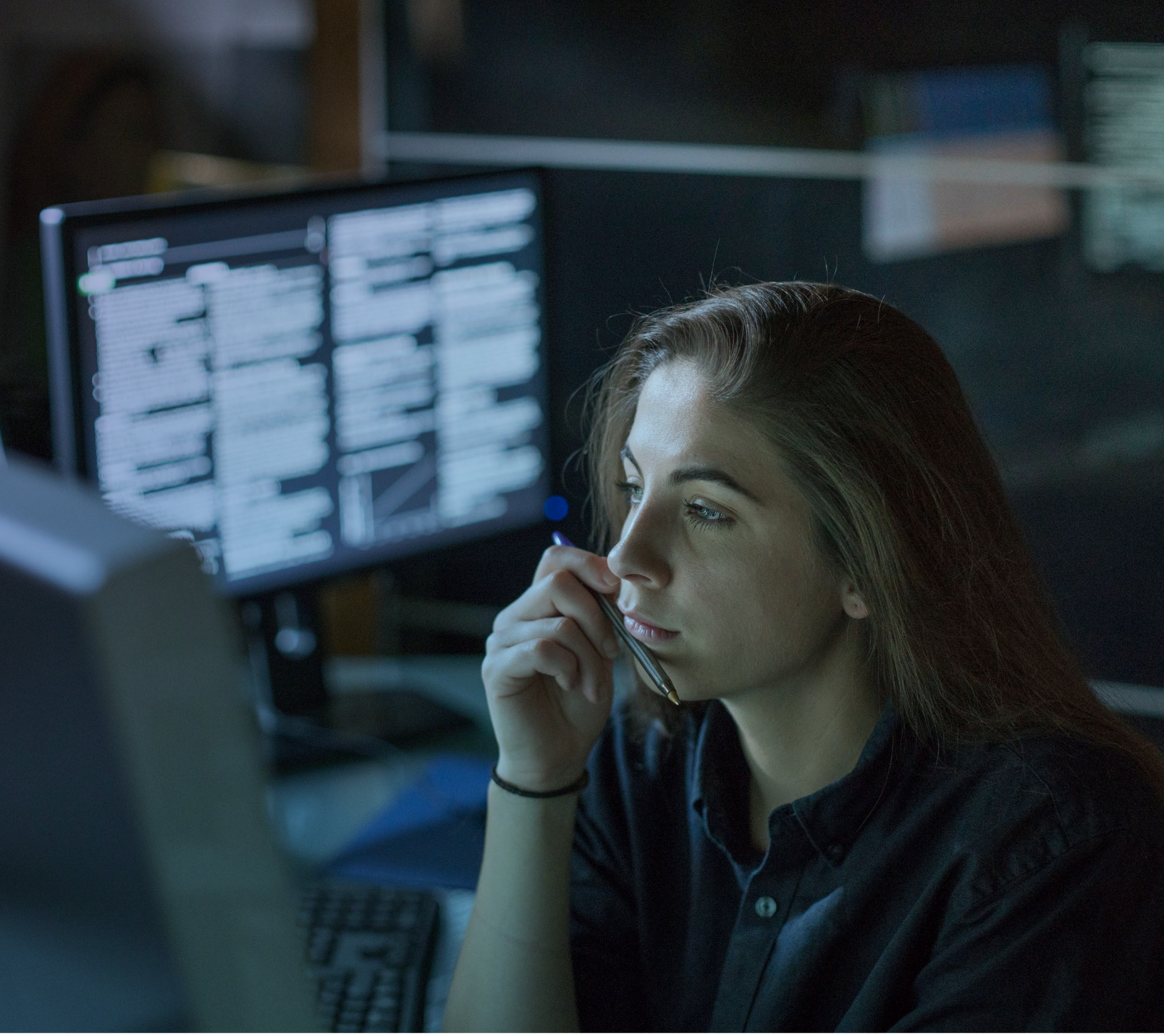


Enable consistent team collaboration for Cloud Security with Zscaler Workload Posture

zscaler™

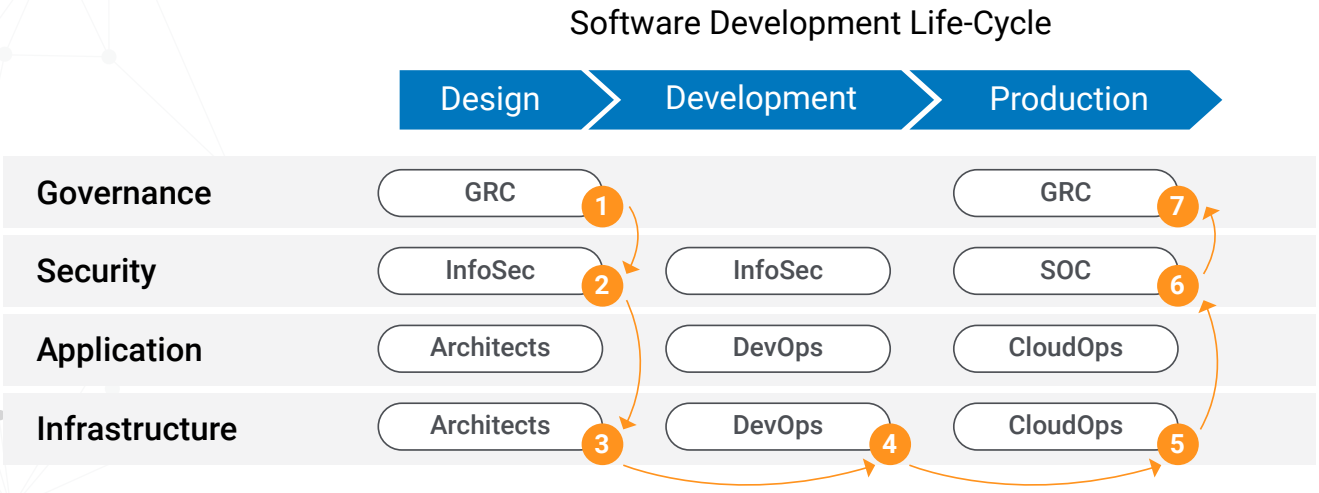
The benefits of digital transformation are immense, compelling many businesses to aggressively move workloads to public cloud platforms, leaving IT with the challenge of adequately securing these environments.

Reducing misconfigurations, monitoring risk of data exposure, and preventing unauthorized access are foundational for ensuring the security and compliance of cloud applications and data. As criminals become more sophisticated in their abilities to exploit cloud misconfiguration vulnerabilities, security teams need a smarter approach to securing team collaboration, in order to prevent breaches and eliminate data exposure.

To begin, securing cloud deployments requires collaboration between the executive team (CISO), InfoSec, Security Operations Center (SOC), and application development (AppDev) teams. While the InfoSec team is responsible for setting the corporate security standards, all other teams play a significant role in implementing these security and compliance standards.

For instance, successfully modernizing your organization's cloud security posture in unison across all teams involved typically includes the following steps:

1. CISO lays down a roadmap to secure multiple clouds
2. GRC (Governance, risk management and complaince team) specifies required compliance frameworks
3. InfoSec defines corporate information security standards
4. Cloud architects create secure application architecture configurations
5. DevOps deploys cloud infrastructure
6. CloudOps fixes discovered cloud services, identities, or access misconfigurations
7. SOC monitors security posture
8. GRC provides evidence of continuous compliance



Executive team, CISO:

If the organization uses multiple cloud platforms, such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure, the CISO must have visibility across all of them, including what workloads are running on them and the details on how each is secured. The CISO will then use this information for a variety of purposes, including:

- Making sure the organization's security and compliance standards are being met in the cloud
- Reducing complexity by identifying redundant, obsolete, and functionally narrow security tools
- Implementing consolidated, integrated, and modern cloud-based security solutions

GRC: Risk posture and compliance frameworks

GRC teams specify required industry compliance frameworks (based on industry benchmarks, laws, and regulations). Depending on industry and location(s), some organizations may have multiple compliance and security frameworks to operate within.

InfoSec: Corporate standard

The InfoSec team is responsible for defining a set of "must-have" security and access policies for their organization, including cybersecurity benchmarks and additional company-specific policies. Cloud security tools like Zscaler's Workload Posture help the infosec team discover and gain 360-degree visibility into all assets, identities, crucial databases, entitlements, configurations, and associated security risk in a single, analytics-rich interface. It also offers the ability to add private benchmarks that customers can track and enforce.

Cloud Architects: Configuration guides

Architects design cloud infrastructure by taking into account best practices to create secure configuration guides for CloudOps teams. Zscaler Workload Posture offers 2700+ pre-built and mapped cloud security best practices with detailed definitions to guide configurations and audits, including remediation steps.

DevOps: Deploy infrastructure

With so much cloud infrastructure now deployed automatically, the infrastructure management team, or DevOps team, must scan cloud infrastructure both pre-and post-deployment. Any discovered cloud service or identity misconfigurations need to be fixed prior to production.

CloudOps: Fix misconfigurations

The CloudOps team initiates a scan immediately after deployment into the production environment, as well as on an ongoing basis. Any discovered identity or service misconfigurations must be fixed quickly on priority, depending on their risk level. Workload Posture offers a dedicated dashboard for the Cloudops team to monitor risk. It easily integrates with current SecOps ecosystems such as ServiceNow, Zendesk, or Splunk so that the SecOps team can act immediately and effectively.

SOC: Continuous monitoring

SOC teams should scan production environments continuously to validate any undesired manual configuration changes. SOC teams monitor for policy deviations and escalate recently discovered, critical security or compliance violations. Workload Posture helps the SOC team enforce security and perform compliance checks at the development stage to keep up with DevOps deployment speed.

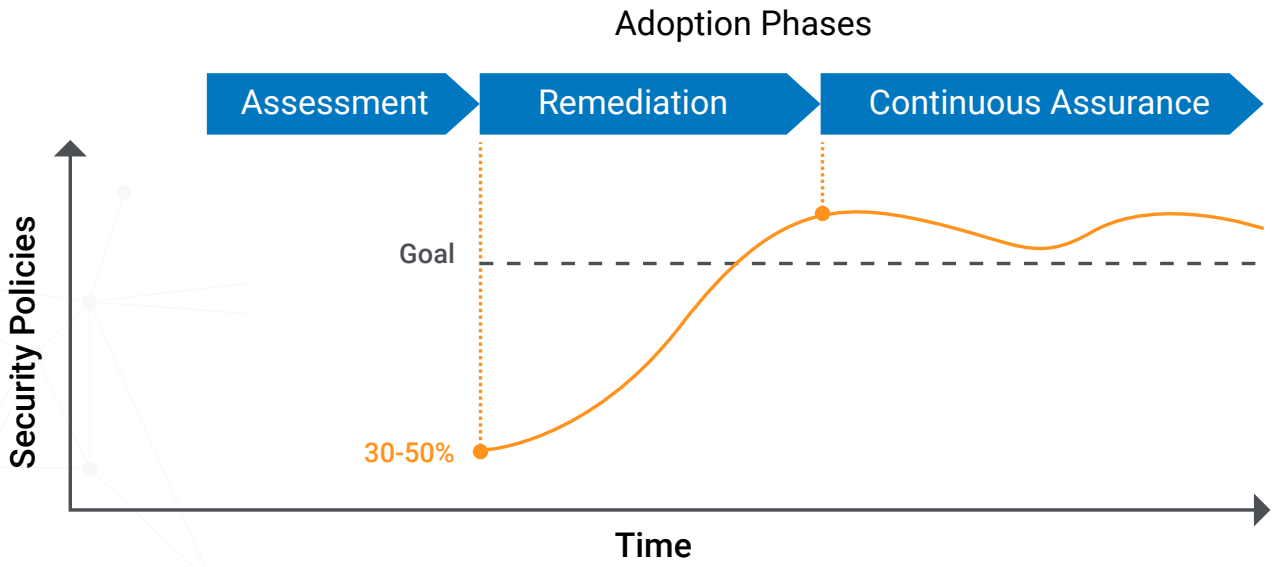
GRC: Compliance evidence

Compliance teams have access to daily monitoring results and can provide these reports as proof of continuous compliance to regulators and auditors.

Adoption steps

Assess your security posture

Companies use Workload Posture Management solutions to provide compliance evidence based on common cybersecurity frameworks such as CIS or NIST. Moreover, Workload Posture Management is used in regulated industries as proof of adhering to industry-specific compliance to standards such as HIPAA for healthcare, SOC 2 for ISVs, PCI DSS for e-commerce, ISO 27001 for enterprises with international operations, and FFIEC for financial services, and so on.



Organizations can use Zscaler Workload Posture solutions to assess existing cloud infrastructure to determine its current security posture. Typically, a project is initiated to identify "must-have" security policies in collaboration with the Information Security (InfoSec) team and initiate remediation activities.

Remediate to achieve the goal

Remediation requires specialized CloudOps team training on cloud security best practices and new configuration requirements. Remediations are first validated in pre-production environments to ensure that new cloud infrastructure configurations won't break applications or impact app performance.

Dev/Test and pre-production environments are rebuilt per new configurations and permissions aligned with the desired security posture. As a result, the security posture improves to meet and/or exceed goals.

Continuous Assurance

After remediation, CloudOps teams take responsibility for ongoing security, identity access management, and compliance assurance. They monitor security posture in the production environment daily to make sure that last-minute fixes or updates do not introduce any misconfigurations.

Security and access management tools are also used on an ongoing basis in Dev/Test and pre-production environments to validate the accuracy of configurations and permissions before deploying new application releases into production environments.

Security operations teams (SOC) should add security posture monitoring to their dashboards and escalate quickly any critical misconfigurations of cloud services or identities discovered in the production environment.

About Zscaler Workload Posture

Zscaler Workload Posture automates visibility, governance, and compliance across AWS, Azure, GCP, and Microsoft 365,allowing organizations to manage asset configurations, access permissions, sensitive data protection, and ensure cloud compliance. Moreover, Zscaler Workload Posture helps organizations create their private benchmarks, supports large-scale application environments, and allows rapid adoption of DevSecOps.

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**.

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