

Cloud Security Posture Management

SUMMARY

Our Cloud Security Posture Management (CSPM) services gain visibility and automated control into their cloud environment as these become increasingly important for business operations. Our CSPM services provide the ability to deploy, operate, and implement best security practices to your cloud environment to ensure security and maintain compliance.

FEATURES

- Operates with AWS, Azure, GCP, and OCI (Oracle) cloud environments.
- “Security Check-Up” assessment to provide baseline understanding of your cloud environment, establish an asset inventory, and prioritize key security issues.
- Continuous assessment of your cloud environment leveraging API integration
- Customizable ruleset to comply with established rulesets and the the flexibility to create specialized policies for unique security needs.
- Automatic remediation mechanisms to ensure alignment with security and compliance requirements.
- real time visualization and reporting to allow for understanding of environment and cloud resource interactions.



VISIBILITY

Enterprise cloud environments are often rapidly changing, while using 1 or more different cloud providers. Traditional network visibility tools are not well suited to maintaining visibility into the cloud, leading to the creation of untracked cloud assets, and uncertainty about the environment architecture. Our Security Check-up assessment, and continuous assessment services allow you to see what is in your cloud environment, providing a full inventory of assets, users, and data.

MONITORING

The constant evolution of cloud environments necessitates 24/7 monitoring for vulnerabilities, misconfiguration, or unauthorized activity. Our CSPM solution goes beyond traditional network monitoring, providing real-time alerting and monitoring to provide constant oversight for your cloud environment. We ensure immediate automated interventions for common issues while more complex incidents are escalated for expert analysis.

COMPLIANCE

Enjoying the benefits of cloud computing: flexible architecture, rapid scaling, and ease of use can often conflict with the needs of security regulations or industry standards. Our automated policy and configuration monitoring and enforcing allows you to align cloud usage with business risk and security requirements to assist with compliance required frameworks including PCI-DSS, HIPAA, HiTrust, NIST, and GDPR.