Your Cloud Security Posture Management Assessment

In the shared security model of the public cloud, you're responsible for the security and compliance implications of resource configurations. This can be especially challenging in a decentralized cloud environment with users capable of configuring resources rapidly.

Public cloud transformation has changed how you approach cloud security posture management (CSPM).

Take this assessment to find out if your organization's cloud posture management meets the following security challenges.

Sharing responsibility of cloud security between different teams throughout the organization

- ☐ Are your IT security teams working with engineering to understand how cloud resources are configured?
- ☐ Are your infrastructure and operations teams informed about cloud security policies?
- ☐ Do your cross-functional teams meet regularly to review your cloud security posture?

Detecting configuration errors in a distributed and complex cloud environment

- ☐ Are you able to visualize configurations across all public cloud platforms and environment types?
- ☐ How do you know if configurations in your environment affect compliance with regulatory standards (e.g., GDPR, PCI, HIPAA)?
- ☐ Can you detect configuration errors, compliance violations, or security vulnerabilities in real time?

Prioritizing configuration errors based on severity

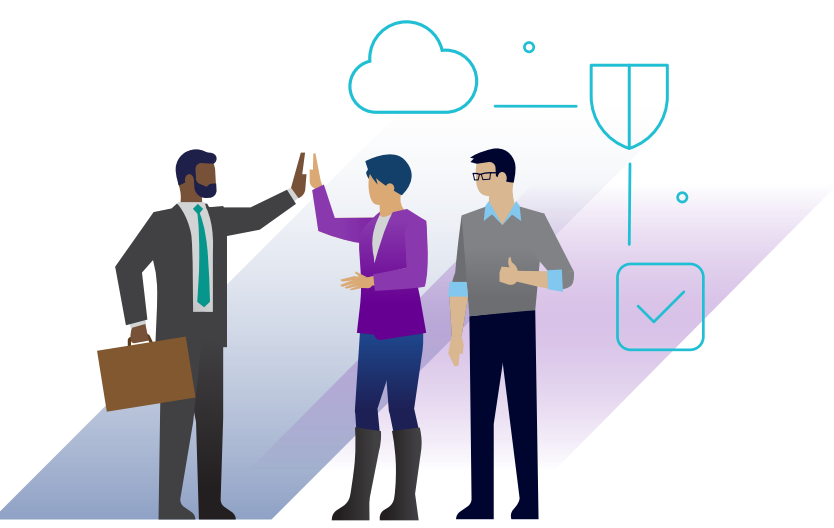
- ☐ Are you able to understand how individual configuration errors can impact other resources in your public cloud environment?
- ☐ Can your teams sort through the noise of your cloud providers' native monitoring notifications and prioritize configuration errors based on severity?
- ☐ Do your teams have the context and information they need to remediate a configuration error?

Ensuring teams adhere to standards for secure cloud configurations

- ☐ Have you established cloud configuration governance policies and role-based access controls to keep your environment secure and compliant?
- ☐ Are you able to automatically alert the relevant stakeholders when policies are violated?
- ☐ Have you implemented automatic remediation for your most common configuration errors?

Integrating cloud security posture management into day-to-day operations

- ☐ Have you evaluated the development pipeline to identify opportunities to incorporate configuration security checks without disrupting productivity?
- ☐ Have you communicated these processes to your development teams?
- ☐ Are you using key performance indicators (KPIs) to measure your cloud security posture and identify opportunities to improve your processes?



If you checked all of the boxes in this security assessment, your cloud posture management is secure. But if you didn't, you may need VMware Aria Automation™ for Secure Clouds. Test-drive the free tier to see how VMware Aria Automation for Secure Clouds allows you to add a cloud account and a Kubernetes instance.

Try the Free Tier

Item No: **1703106aq-info-cld-sec-pstr-mgmt-asmt 1/23**