vmware

Your Cloud Security Posture Management Assessment

In the shared security model of the public cloud, customers are 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 their approach to cloud security posture management (CSPM). Is your organization's cloud security posture effectively managed? Take this assessment to find out.

Challenge:

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 IT security teams working with engineering to understand how cloud resources are configured?
- ☐ Are your IT security teams working with engineering to understand how cloud resources are configured?

Did you know that organizations that move towards a DevSecOps approach are more likely to detect a misconfiguration within a day of the error occuring? Learn how to bring these teams together here.

Challenge:

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 envionment affect compliance with the regulatory standards (e.g. GDPR, PCI, HIPAA)?
- ☐ Can you detect configuration errors, compliance violations, or security violations in real-time?

Want to be able to detect 95% of security violations in less than 6 seconds of change notification? Learn more here.

Challenge:

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 ave the context and information they need to remediate a configuration error?

Challenge:

Ensuring teams adhere to standards for secure cloud configurations

- ☐ Have you evaluated the development pipeline to identify opportunities to incorporate configuration security checks without disrupting productity?
- ☐ Are you able to automatically alert the relevant stakeholders when policies are violated?
- ☐ Have you implementd automatic remediation for your most common configuration errors?

VMware Aria Automation for Secure Clouds state can help you improve compliance with support for over 20 regulatory standards.

Challenge:

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 productity?
- ☐ Are you able to automatically alert the relevant stakeholders when policies are violated?
- ☐ Have you implementd automatic remediation for your most common configuration errors?

If you checked all of the boxes in this security assessment, great job!

If you didn't, test drive our cloud configuration security platform by creating a VMware Aria Hub Free Tier account, which allows you to manage a cloud account and a Kubernetes cluster.

Learn more today.

vmware