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 occurring? Learn how to bring these teams together here.

Challenge: Detecting configuration errors in a distributed and complex cloud environment

- Are you able to visualize cloud configurations across all public cloud platforms and resource types?
- Do you know if configurations or your environment affect compliance or regulatory violations (e.g. GDPR, ROC, HIPAA)?
- Can you detect and respond to security, 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

- Can your teams sort through the noise of your cloud provider’s 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 evaluated the development pipeline to identify opportunities to incorporate configuration security checks without disrupting productivity?
- Are you able to automatically alert the relevant stakeholders when specific policies are violated?
- Have you implemented automatic remediation for your most common configuration errors?

Have you evaluated the development pipeline to identify opportunities to incorporate configuration security checks without disrupting productivity?

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 impact of introducing configuration security checks and remediation processes?
- Are you able to visualize configuration security checks and remediation processes?
- Have you implemented configuration security checks and remediation processes for your most common configuration errors?

Detecting configuration errors in a distributed and complex cloud environment

- Are you able to visualize configurations across all public cloud platforms and environment types?
- Can your teams sort through the noise of your cloud provider’s 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?

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 Tier account, which allows you to manage a cloud account and a Kubernetes cluster. Learn more today.

Copyright © 2022 VMware, Inc. All rights reserved. VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 VMware and the VMware logo are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. VMware products are covered by one or more patents listed at vmware.com/go/patents.