ALIGNED
TECHNOLOGY GROUP

SOLUTION BRIEF

AWS Cloud Security Posture Assessment

Aligned Technology Group offers a comprehensive Cloud Security Posture Assessment (CSPA) that provides you with automated visibility you expect to figure out how your AWS environment is configured and how it measures up against industry specific cybersecurity frameworks, regulations, and standards.

Highlights

- Cloud Security Posture Management (CSPM) is a fundamental activity that introduces the necessary detective safeguards to protect your business-critical workloads and non-public data.
- Trust Aligned Technology Group to perform a Cloud Security Posture Assessment (CSPA) of your environment and we'll help you implement continuous Cloud Security Posture Management (CSPM).
- Check out Aligned Technology Group's Cloud Architecture Risk Analysis (Cloud ARA) if you need infrastructure diagrams and a deeper understanding of your cloud security posture and strategy.

Overview

According to a Cloud Security Alliance 2021 report, the primary causes of cloud misconfiguration are a lack of knowledge or expertise in cloud security best practices and lack of security visibility and monitoring.

Rely on an Aligned Technology Group delivered AWS Cloud Security Posture Assessment (CSPA) to:

1.Train your team to perform proactive and continuous Cloud Security Posture Management (CSPM).

2.Obtain visibility into how your AWS environment is configured and secured and evaluate the extent to which your environment is well-architected.

3.Identify high risk security misconfigurations that might lead to inadvertent data exposure or public cloud account takeover.

4.Received detailed remediation instructions describing how to fix issues using the AWS CLI or the management console.

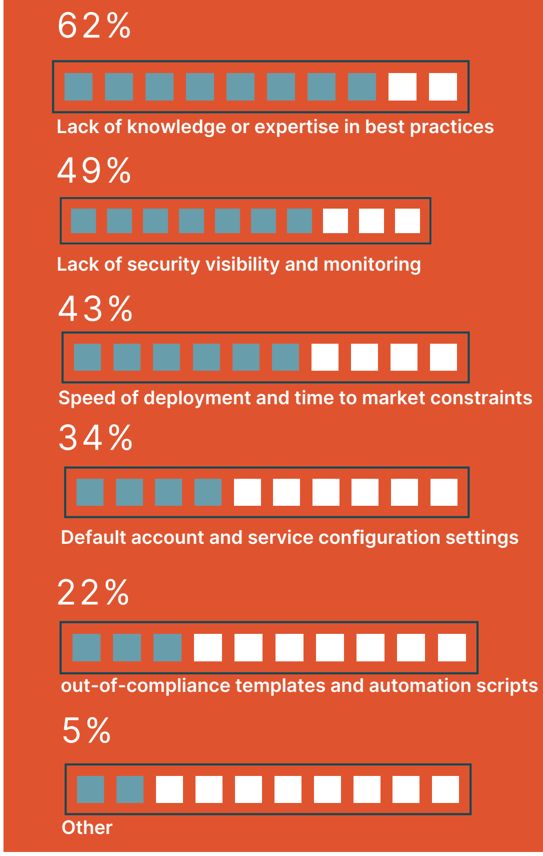
5.Confirm that your public cloud infrastructure is secure and that it complies with relevant regulatory requirements and industry standards including the following:

- AWS Well-Architected Framework
- Center for Internet Security AWS Foundations Benchmarks
- NIST Cybersecurity Framework
- HIPAA 45 CFR 164
- HITRUST CSF
- NIST 800-53
- PCI-DS S
- SOC 2

SECURITY SPECIALISTS

Causes of Cloud Misconfiguration

According to the Cloud Security Alliance the primary causes of cloud misconfigurations lack of knowledge or expertise in cloud security best practices and lack of security visibility and monitoring.



Deliverables

1.Comprehensive report that reflects your AWS environment's current state security posture along with risk-based, actionable, and detailed recommendations and remediation instructions.

2.Option to have Aligned Technology Group remediate business critical issues.