ALERT LOGIC®
Security. Compliance. Cloud.

turbot

SOLUTION OVERVIEW:

SECURING CLOUD WORKLOADS WITH TURBOT & ALERT LOGIC

SECURING AND PROTECTING CLOUD WORKLOADS

Organizations using cloud services gain significant benefits from the security capabilities built into the platform; however, not everyone takes advantage of these capabilities. In many cases, development teams make early tradeoffs to forego security in favor of project velocity and then fail to come back to properly secure the infrastructure before production deployment.

To effectively secure cloud workloads, organizations must find ways to ensure control without impeding developer productivity. Focusing on these three key areas will enable your organization to create an environment where security is automated:

- Automate environment setup to systematize AWS best practices.
- Use guardrails to ensure environment configurations do not drift over time and that applications and operating systems are continuously patched.
- Monitor your environment for attacks and indications of suspicious activity.

Alert Logic and Turbot can help meet these requirements across these three phases.

ALERT LOGIC WAS BUILT FOR AWS

Alert Logic solutions combine cloud-based software and threat analytics with expert services to assess, detect and block threats to applications and other workloads. Protection extends to all layers of your web application and infrastructure stack to defend against a broad range of attacks -- including hard-to-detect web application attacks such as SQL injection, path traversal and cross-site scripting as well as advanced malware/command to control, brute force -- while also helping you comply with mandates like PCI, HIPAA and SOX COBIT. Designed for cloud and hybrid environments, Alert Logic solutions use API-driven automation and integration with cloud platforms and DevOps tools.

TURBOT: AUTOMATE YOUR CLOUD, ELEVATE YOUR TEAM

Turbot delivers Software Defined Operations for the enterprise cloud with automated guardrails that ensure your cloud infrastructure is secure, compliant, scaleable and cost optimized. Turbot's SDOps platform enables your cloud team to focus on delivering higher-level value while your application teams remain agile through use of native AWS tools. Turbot will ensure your internal teams are always following best practices and implementing security controls properly (including the Alert Logic deployment) without sacrificing velocity.

	ALERT LOGIC	TURBOT
Initial Deployment	• Scan the environment to ensure applications and operating systems are at recommended patch levels and configured properly	• Fully script best practices into a deployment runbook • Scan the environment to ensure instances and AWS configuration is consistent with best practices
On-going Monitoring	• Monitor AWS configuration and application and operating system patch levels and configuration	• Monitor configuration changes, drift, and operating system patch levels
Threat Detection & Response	• Monitor network and application-level traffic to identify attacks • Review logs to detect indicators of compromise	• Monitor Alert Logic incident notifications, and automatically remediate for specific incident types

PATCH VULNERABILITIES BEFORE THEY CAN BE EXPLOITED

Alert Logic and Turbot continuously monitor your environment to verify OS patches and configurations are up to date. Turbot can automatically perform CIS level OS patching and ensure that your network configuration does not drift over time. When Alert Logic discovers a vulnerability, Turbot can isolate the instance until your team has a chance to perform forensic analysis of the compromised assets.

AUTOMATICALLY RESPOND TO WEB APPLICATION ATTACKS

Web application attacks, like SQL Injection, are increasingly used to compromise your environment and exfiltrate sensitive data. Alert Logic Cloud Defender is designed to detect these attacks and other activities like reconnaissance or application exploits. Turbot's network guardrails make it easy for development teams to apply network security best practices using predefined AWS security groups.

CONCLUSION

Cloud platforms enable increased operational velocity, and in many cases, a more cost-effective infrastructure. However, securing and protecting these environments is a shared responsibility, and organizations using the cloud should ensure their deployments leverage best practices, and monitor these environments for attacks. Alert Logic and Turbot can help your organization secure and protect your environment without creating additional overhead on your teams, and in many cases, taking on the responsibility so your teams can focus on creating business value.