ALERT LOGIC® | aws

TECHNICAL BRIEF

EXPERT-ENABLED SAAS SECURITY BUILT FOR AWS

aws partner network

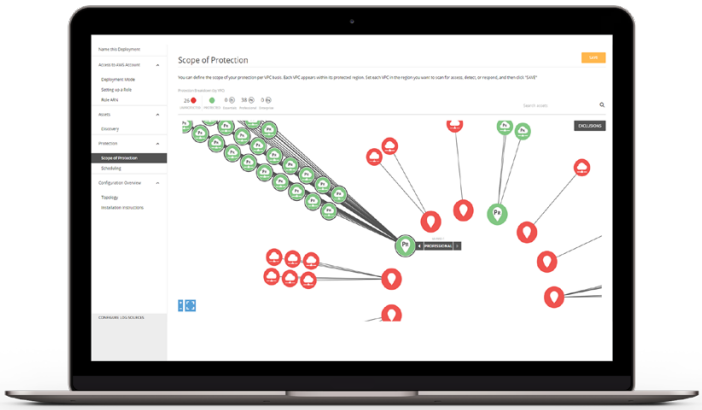
Advanced Technology Partner

- Security Competency
- Containers Competency
- SaaS Partner
- Marketplace Seller

Evolving threats, expanding compliance risks, and resource constraints require a new approach. Alert Logic seamlessly connects an award-winning security platform, cutting-edge threat intelligence, and expert defenders — to provide the best security and peace of mind to your business 24/7.

Alert Logic protects your Amazon Web Services (AWS) workloads by defending your cloud, applications, and infrastructure. With API-driven automation and DevOps templates for AWS, Alert Logic provides agile security and compliance that scales..

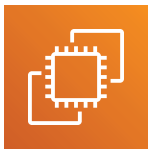
- **Add security experts** to your team overnight without hiring staff
- **Get expert incident analysis** and live notifications of active attacks in 15 minutes
- **Visualize all assets** in your AWS environment
- **Easily track and analyze** risk levels, threat details, potential impact, and detailed remediation recommendations
- **Protect your container environment** for AWS Elastic Container Services ECS & EKS, AWS-deployed Docker & Kubernetes, Elastic Beanstalk and CoreOS
- **Demonstrate compliance** with reporting and focused security controls designed to meet your audit and regulatory needs
- **Simplify with one service** that works across multiple cloud and on-premises environments



Visualize impact with dynamic topology mapping

SEARCH ALERT LOGIC IN THE AWS MARKETPLACE aws marketplace

COMPREHENSIVE VISIBILITY



AMAZON EC2 AND AWS ELASTIC BEANSTALK

A lightweight agent is deployed to detect a wide array of attack methods for security threats lurking in your network traffic and log data, including exploits in web app frameworks, containers, app stack components, and OWASP Top 10.

AWS CONTAINER SERVICES

Alert Logic has the industry's only network intrusion detection solution and log management for containers - with support for AWS, hybrid, and on-premises environments. Detect and visualize threats in real-time for any workload in any container (Docker, Kubernetes, Elastic Beanstalk, Elastic Container Service, Elastic Kubernetes Service and CoreOS). Our security professionals watch over your environment 24/7 - so you're never on your own.

AMAZON WORKSPACES

Endpoint protection helps thwart multiple attack techniques that try to compromise Windows endpoints. Our multi-vector attack monitoring and isolation recognizes these techniques and stops them early before any damage is done.

AWS IDENTITY AND ACCESS MANAGEMENT

User behavior anomaly detection (UBAD) for AWS environments detects and alerts on suspicious activity. This capability uses machine learning to help determine a baseline of user behavior and identify changes in the way users access your systems including locations and times of access. Using AWS CloudTrail data, Alert Logic can detect and raise incidents for anomalous user behavior that may impact critical assets in your AWS environment.

AWS CIS BENCHMARKS

The Center for Internet Security (CIS) AWS Foundations Benchmark is a set of guidelines that helps customers secure their AWS cloud environment with step-by-step guidance for implementation and assessment. Alert Logic Configuration checks support both Level 1 and Level 2 of the CIS AWS Foundations Benchmark and provide an easily consumable report in the user interface.

SECURITY INTEGRATED

AMAZON GUARDDUTY

Alert Logic shows you why, where, and how to respond to Amazon GuardDuty findings, while continuously discovering and assessing your AWS configurations to find exposures and provide easy-to-understand actions that prevent future compromises.

SECURITY INTEGRATED (CONT.)

AWS SECURITY HUB

Integration with AWS Security Hub provides a comprehensive view of your security state. Security Hub is a dashboard within the AWS console where you can view findings generated by Alert Logic along with findings from AWS services.

AWS CLOUDTRAIL

AWS CloudTrail records actions taken by a user, role, or AWS service as events. Alert Logic treat API activity data as any other data source to capture and manage. Alert Logic integrates with AWS CloudTrail to collect API activity data within an AWS account and then combines the data with log data from other applications and systems.

AWS SECURITY SERVICES & TOOLS

Alert Logic consumes findings from various AWS security services including AWS IAM Access Analyzer, Amazon Inspector, and AWS Config, and reports them as remediations and exposures within the Alert Logic console. This gives customers a single pane of glass to view AWS authentication, account configuration issues, config rule violations along with the exposures and vulnerabilities identified by Alert Logic's service.

AWS CONTROL TOWER

Alert Logic and AWS are bringing automated Managed Detection and Response (MDR) deployment into AWS Control Tower managed accounts. With this new capability, AWS Control Tower users can seamlessly deploy and configure Alert Logic MDR using their existing AWS Control Tower setup, reducing the number of steps required for deployment and ensuring consistency across accounts.

DEVOPS READY

AWS CLOUDFORMATION

From agent deployment to configuration of AWS services to allow Alert Logic's asset discovery and detection technologies to work, Alert Logic provides sample cloud formation scripts for customers to adapt to their workflow.

AWS CLOUDTRAIL

Alert Logic integrates tightly with AWS CloudTrail to detect changes to your workloads and automate changes in AWS services. Alert Logic detects those changes and then updates configuration checks accordingly.

GITHUB

Configuration of AWS services, deployment of Alert Logic's sensors, including deployment of our container agent directly into your container environment, and more are all available via our public GitHub.

AWS SHARED RESPONSIBILITY MODEL

YOUR ROLE IN SECURING YOUR AWS ENVIRONMENTS

Security and compliance is a shared responsibility. Cloud computing and AWS have changed the way enterprises manage their data and other operational burdens but organizations still struggle when extending security to the cloud. While AWS protects the physical security of the cloud and provides certain protections, you are still responsible for deploying, configuring, and maintaining the security of everything within your cloud.

Alert Logic provides the managed intrusion detection, log management, advanced event correlation, and web application protection necessary to help meet your share of security responsibilities for security and compliance posture.

Alert Logic helps you stay ahead of your responsibility with asset visibility, vulnerability assessment, threat detection and response, and web application security, all at optimal cost. You also get:

- Expert incident analysis, threat intelligence, and a modern, always up-to-date platform
- Managed intrusion detection to detect threats lurking in your network traffic
- Log management and review to meet compliance requirements
- Advanced event correlation to identify suspicious behavior
- Configuration management to uncover vulnerabilities hidden within your application stack

ALERT LOGIC®