SOLUTION BRIEF

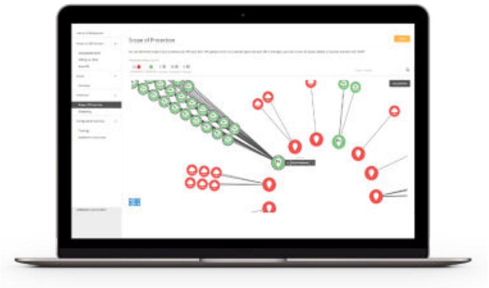
Expert-Enabled SaaS Security Built for AWS

Protecting Your Workloads with Fortra's Alert Logic MDR®

Evolving threats, expanding compliance risks, and resource constraints require an innovative approach to security. Fortra's Alert Logic seamlessly connects an award-winning security platform, advanced threat intelligence, and expert defenders to provide the best security and peace of mind to your business 24/7. We protect 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 scalable, agile security and compliance:

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

- Security Software Competency
- L1 MSSP Software Competency
- Containers Software Competency
- AWS Marketplace Seller
- Public Sector
- Amazon Linux Ready
- AWS Control Tower Ready
- AWS Outposts Ready



Visualize impact with dynamic topology mapping

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, from Docker to AWS Fargate and everything in between. Our security professionals monitor your environment 24/7 so you're never on your own.

Amazon Workspaces

Endpoint protection helps thwart multiple attack techniques trying to compromise Windows endpoints. Our multi-vector attack monitoring and isolation recognizes these techniques and stops them early before damage occurs.

AWS Identity and Access Management

User behavior anomaly detection (UBAD) for AWS environments detects and alerts you of suspicious activity. This capability uses machine learning to help determine a baseline of user behavior and identify changes in how 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 Foundations Benchmarks

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

Integrated Security

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 uncover exposures and provide easy-to-understand actions that prevent future compromises.

AWS Security Hub

AWS Security Hub is a dashboard within the AWS console where you can view both findings generated by Alert Logic and AWS.

AWS CloudTrail

AWS CloudTrail records actions taken by a user, role, or AWS service as events. Alert Logic treats 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 and Tools

Alert Logic consumes findings from various AWS security services including AWS IAM Access Analyzer, Amazon Inspector, and AWS Config, and then 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, and config rule violations along with the exposures and vulnerabilities identified by Alert Logic's service.

AWS WAF

Alert Logic's Automated Intelligent Response can initiate blocks on AWS WAF.

AWS Control Tower

Alert Logic and AWS bring automated managed detection and response (MDR) deployment into AWS Control Tower managed accounts. With this capability, AWS Control Tower users can seamlessly deploy and configure Fortra's Alert Logic MDR® with their existing AWS Control Tower setup, reducing the number of steps required for deployment and ensuring consistency across accounts.

AWS Network Firewall

Collect, parse, and correlate AWS Network Firewall activity within the Alert Logic console for enhanced visibility and threat detection coverage.

DevOps Ready

AWS CloudFormation

From agent deployment to configuring AWS services to allow Alert Logic's asset discovery and detection technologies to work, we provide sample cloud formation scripts so you can adapt your workflow.

AWS CloudTrail

Alert Logic integrates tightly with AWS CloudTrail to detect changes to your workloads and automate changes in AWS services. After detecting any changes, we update configuration checks accordingly.

GitHub

Configuring AWS services, deploying Alert Logic's sensors, including deployment of our container agent directly into your container environment, and more is available through our public GitHub.

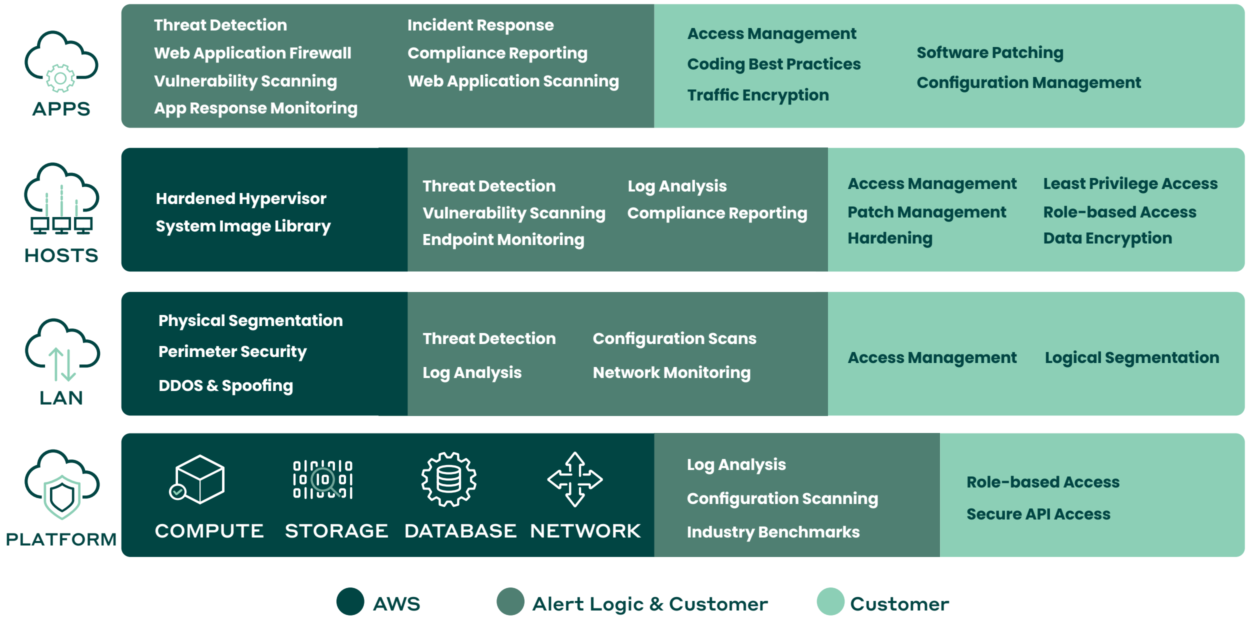
AWS Shared Responsibility Model

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 do struggle when extending security to the cloud. While AWS protects the physical security of the cloud and provides certain protections, you have responsibility for deploying, configuring, and maintaining the security of everything within your cloud.

Fortra's Alert Logic MDR provides the managed intrusion detection, log management, advanced event correlation, and web application protection necessary to help meet your share of responsibilities for security and compliance posture. We help you stay on top of your responsibility with asset visibility, vulnerability assessment, threat detection and response, and web application security, all at an optimal cost. With Alert Logic, you also receive:

- Expert incident analysis, threat intelligence, and a modern, 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



APPS		Threat Detection Web Application Firewall Vulnerability Scanning App Response Monitoring Incident Response Compliance Reporting Web Application Scanning	Access Management Coding Best Practices Traffic Encryption Software Patching Configuration Management
HOSTS	Hardened Hypervisor System Image Library	Threat Detection Vulnerability Scanning Endpoint Monitoring Log Analysis Compliance Reporting	Access Management Patch Management Hardening Least Privilege Access Role-based Access Data Encryption
LAN	Physical Segmentation Perimeter Security DDOS & Spoofing	Threat Detection Log Analysis Configuration Scans Network Monitoring	Access Management Logical Segmentation
PLATFORM	COMPUTE STORAGE DATABASE NETWORK	Log Analysis Configuration Scanning Industry Benchmarks	Role-based Access Secure API Access

● AWS ● Alert Logic & Customer ● Customer

For more information, please visit **alertlogic.com**

About Fortra

Fortra is a cybersecurity company like no other. We've created a simpler, stronger, and more straightforward future for our customers. Our trusted experts and best-in-class portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally for cybersecurity that prevails. Learn more at fortra.com.

FORTRA
Fortra.com