FORTRA

SOLUTION BRIEF (Alert Logic)

Alert Logic for Amazon Web Services

Managed Detection and Response for AWS

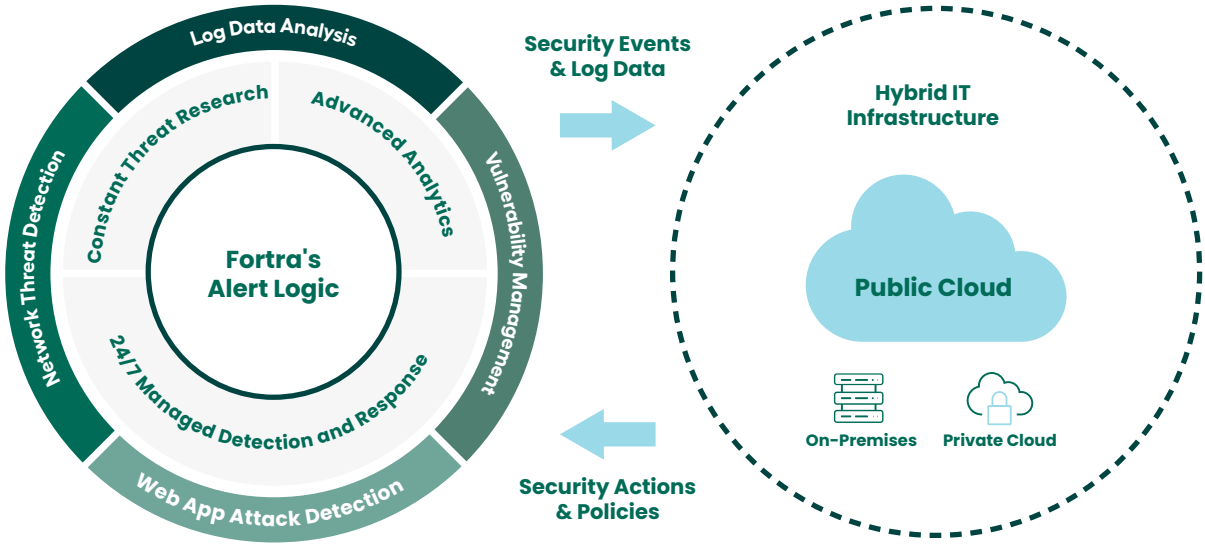
Few things are as important to your business as securing your sensitive data. Protecting your brand, evolving your products and services, growing your customer base, and maintaining your competitive advantage depend on protecting this data. In the past, when an individual threat actor used "smash-and-grab" methods to steal data, protection strategies were straightforward. Today's threat landscape is more complex. Threat actors are more organized, using multi-vector targeted attacks to penetrate your environments, conceal their presence, and steal as much of your data as possible.

Building a comprehensive security platform to protect against these attackers by integrating multiple point products and training your staff to install, configure, and manage them 24/7 is complex and expensive. If your sensitive data is both in on-premises data centers and the cloud, you may need different solutions for each environment, increasing the initial investment and ongoing costs required to maintain them effectively.

It is clear that meeting today's security challenges using yesterday's products is not possible. You need a security strategy that allows you to stay ahead of threat actors no matter where your sensitive data resides. The right strategy is one that moves you from being siloed, reactive, and technology centric to being integrated, proactive, and knowledge centric in your approach to securing your data.

Fortra's Alert Logic Delivers Comprehensive Security Strategy for AWS

Alert Logic is a fully managed cloud-based suite of security and compliance solutions, delivered as-a-service for AWS, on-premises, and hybrid infrastructures. Our experts make it easy for any organization to reach their security goals in days to weeks, not months to years. With no large capital investment needed, products to purchase, lengthy implementation, or heavy training requirements, Alert Logic is the most effective way for an organization to secure their assets and data using our simple subscription model.



Powered by our threat data analytics platform and security intelligence team, Alert Logic helps organizations:

Identify and Mitigate Network Threats

With real-time threat monitoring and proactive incident identification, our security experts alert organizations quickly when an attack is detected in AWS environments. We provide 24/7 monitoring of threats that could compromise data or impact system availability on AWS — from account to instance.

Detect Security Issues and Analyze Events from Log Data

Certified security experts analyze log data from your instances, AWS CloudTrail, Amazon S3, Elastic Load Balancer, and other data sources to identify suspicious activity that may indicate a security risk. With Alert Logic, organizations can reduce costs associated with audit preparation, while gaining deeper visibility into activity occurring throughout your AWS environment by automating the collection, aggregation, and normalization of log data across all regions.

Protect Against Web Application Threats

The combination of our signature-based detection and an embedded learning engine provide protection by detecting both known attacks and deviations from your expected application behavior. Web Application Firewall security experts in our Security Operations Center (SOC) manage and monitor your environment 24/7 to ensure your web applications and business in AWS are secure.

Identify Vulnerabilities and Assess Your Security Posture

By providing continuous protection of your AWS environment, auto-discovery of assets, and the impact vulnerabilities, misconfigurations, and security groups changes have, you gain insight into your risk profile and receive actionable intelligence to improve your security and compliance posture. Our integration with AWS APIs, CloudTrail, and Amazon Inspector provide the complete visibility you need to secure your AWS environment.

Comprehensive Container Security at the Network Level

Protect against cyberattacks that target your AWS-hosted containers. Alert Logic container security solutions are designed for real-time detection of known and unknown exploits in AWS-deployed Docker, Kubernetes, Elastic Beanstalk, Amazon Elastic Container Services (ECS), and AWS Fargate.

Correlate Disparate Security Events to Identify High Priority Security Issues

Alert Logic aggregates security events and incidents from CloudTrail and other data sources, creates correlation rules, manages threat intelligence content, and cross-correlates security data to identify high priority incidents that may affect your AWS environment.

Compliance Without Complexity

In choosing Alert Logic, organizations can reduce the burden associated with meeting key compliance requirements across their AWS, on-premises, and hybrid environments. We map to specific mandates, such as PCI DSS, Sarbanes-Oxley, and HIPAA, so customers can be confident that those requirements are fulfilled.

The Alert Logic Difference

Alert Logic addresses many security and compliance challenges for organizations, including:

AWS Shared Responsibility Model

Alert Logic can help you meet AWS Shared Responsibility Model requirements by securing your content, platform, systems, networks, and applications that make use of AWS services. As Alert Logic has AWS security best practices built-in, ensuring you're deploying, configuring, and maintaining security baselines is straightforward.

Centralized Security Management

Whether your datacenter infrastructure is on AWS, on-premises, or both, Alert Logic protects them all and provides a single-user experience, eliminating the need for a different security solution for each type of environment. Additionally, Alert Logic offers integrated security tools to protect your data comprehensively and consistently at several layers of the application stack — network, system, and web application.

Scalable Threat Detection and Response Management

Alert Logic delivers a managed security solution, providing the benefits of a traditional security solution without the cost and complexity of internal deployment and management. It combines advanced technology and security expertise to deliver the features, security content, threat investigation, and contact from our security experts with remediation steps

when a high priority incident is detected. Unlike traditional solutions requiring hardware purchases, implementation of complex software, correlation rule configuration, and internally generated security content, Alert Logic includes everything needed for an effective and easy security solution that scales as your company grows.

Native Public Cloud Security

As Alert Logic is delivered from the cloud, it's a solution you can get up and running quickly, protecting your environments in AWS, on-premises, and hybrid infrastructures.

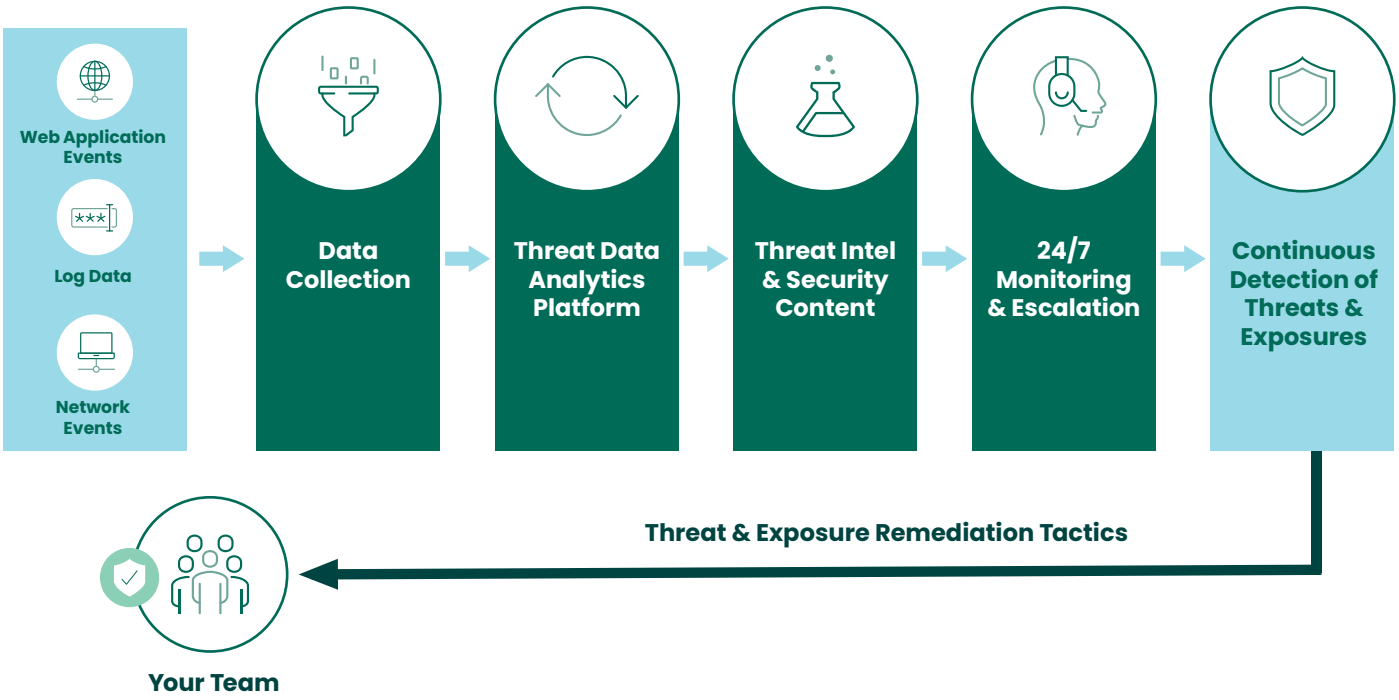
Expert Onboarding and Operationalization

Security investments often go unused or are deployed with partial or default settings — placing businesses at risk while never fully realizing their investment. Our security professionals ensure proper deployment, configuration, tuning, and optimization.

Alert Logic assigns every customer an onboarding project manager (OPM) to administer the entire process and an onboarding team of 20+ specialists including project managers, onboarding engineers, NOC technicians, network and system administrators, security analysts, and product trainers.

Delivering Security Outcomes

When protecting your sensitive data is your top priority, you need an integrated solution designed specifically for that purpose. With Alert Logic, organizations can protect their web applications, platforms, networks, and computing infrastructure with a fully integrated solution from a single vendor they can trust. With our subscription model, Alert Logic not only takes the complexity out of security and compliance, but we also eliminate any frustration and confusion related to purchasing.



Built to Protect Your Sensitive Data

Threat and Exposure Remediation Tactics

Alert Logic combines advanced technology with a team of certified security and compliance experts working 24/7 to keep your data safe and secure, and your environment compliant:

- Protects sensitive data on AWS, on-premises, and hybrid infrastructures with a single solution
- Integrates network, application, and system protection that delivers deeper insight into threats
- Managed and monitored by security experts providing continuous protection
- Subscription model provides protection at a lower cost than traditional security solutions

To learn more about how Alert Logic can help protect your sensitive data, please visit **alertlogic.com**

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.