ALERT LOGIC® | aws

SOLUTION BRIEF:

SIEMLESS THREAT MANAGEMENT BUILT FOR AWS

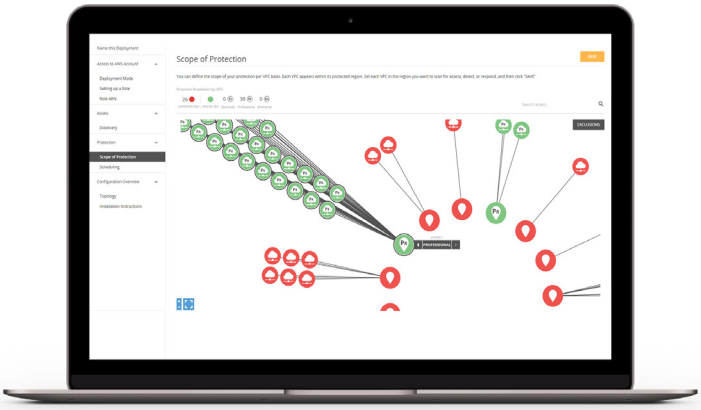
aws partner network

Advanced
Technology Partner

- Marketing and Commerce Competency
- Security Competency
- SaaS Partner
- Marketplace Seller

Alert Logic solutions integrate cloud-based software, analytics and expert services to **assess**, **detect** and **block** workload threats and help you **comply** with mandates like PCI, GLBA, HIPAA, SOX, SOC2, NIST, ISO, COBIT. We focus on threats most relevant to workloads on AWS by defending your full web application and infrastructure stack, including hard-to-detect web app attacks such as SQL injection, path traversal and cross-site scripting. Integrated expert services for detection, blocking and compliance augment in-house security and empower cloud and application professionals. With native API-driven automation and templates for AWS and DevOps tool chains, Alert Logic solutions provide agile security that scales.

- **Focus on the most cloud-relevant threats** with full-stack protection of your web application and infrastructure stack
- **Accelerate production** with API-driven automation and elasticity
- **Add security experts** to your team overnight without hiring staff
- **Preserve application performance** with lightweight agents and auto-scaling support
- **Simplify** with one service that works across cloud and on-premises environments



Visualize impact with dynamic topology mapping

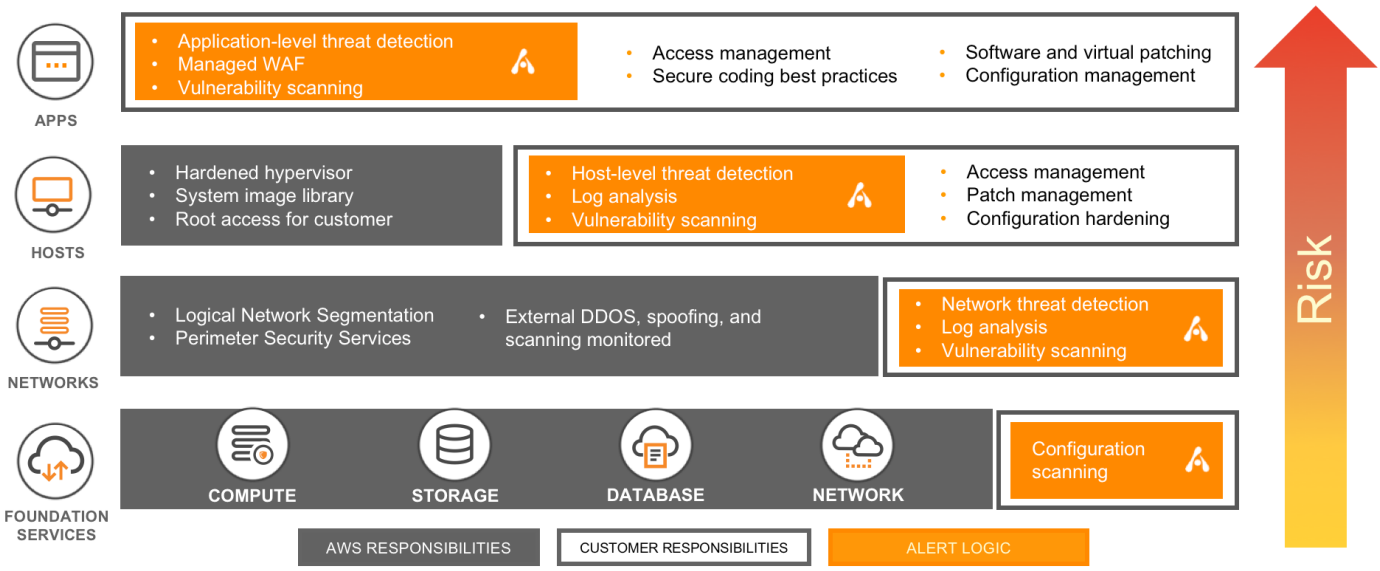
"Alert Logic has a head start in the cloud, and it shows — Alert Logic is an excellent fit for clients looking to secure their current or planned cloud migrations, clients requiring a provider that can span seamlessly between hybrid architectures, and those that demand strong API capabilities for integrations."

– Forrester 2016 MSSP WAVE™ Report

FORRESTER®

FOCUS ON THE MOST CLOUD-RELEVANT THREATS WITH FULL-STACK SECURITY

Security in AWS is a shared responsibility. AWS is responsible for security of the Cloud, such as physical security, instance isolation and protection for foundation services. You are responsible for security in the Cloud, meaning you must secure your applications and data within AWS. When moving from your own data center to cloud computing, your list of security responsibilities may actually be shorter. But that doesn't necessarily make it easier.



AWS invests at scale to secure the network against DDoS and scanning as well as hardening hypervisors against attack. Users can configure hosts that terminate and regenerate from a master image at regular intervals, creating "immutable infrastructure" that prevents host-based threats from retaining a foothold. Cloud innovations such as these are making it more difficult and less profitable for adversaries to attack the lower end of your application and infrastructure stack.

ALERT LOGIC®