ALERT LOGIC® | aws

SOLUTION BRIEF:

SECURITY-AS-A-SERVICE BUILT FOR AWS

aws partner network

Advanced Technology Partner

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

Alert Logic Security-as-a-Service solutions integrate cloud-based software, analytics and expert services to **assess**, **detect** and **block** workload threats and help you **comply** with mandates like PCI, HIPAA and SOX 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

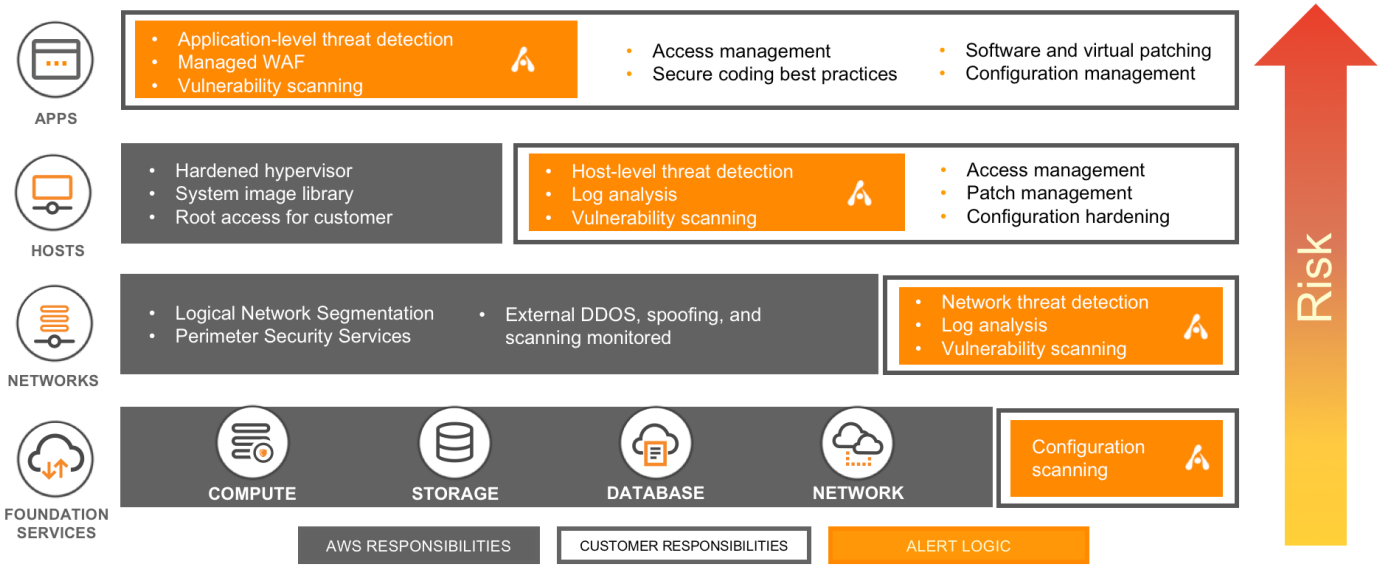
"Alert Logic has a head start in the cloud, and it shows — Alert Logic is an excellent fit for clients looking to secure their current or planned cloud migrations, clients requiring a provider that can span seamlessly between hybrid architectures, and those that demand strong API capabilities for integrations."

– 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.

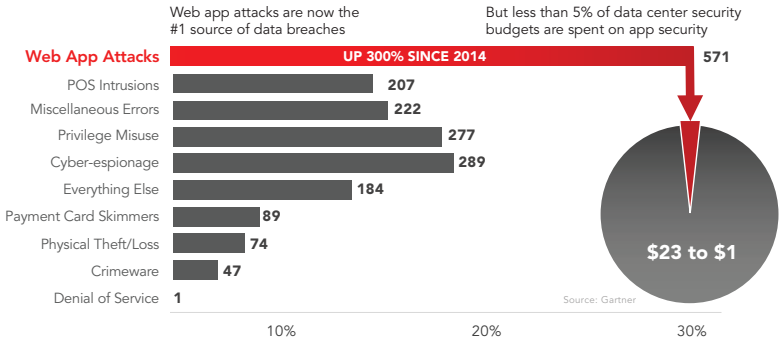


AWS invests at scale to secure the network against DDoS and scanning as well as hardening hypervisors against attack. Users can configure hosts that terminate and regenerate from a master image at regular intervals, creating "immutable infrastructure" that prevents host-based threats from retaining a 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.

While the bottom of the stack is hardening, the top is softening. Businesses are increasingly dependent on inherently vulnerable custom web applications.

Accelerated by a potent mix of hybrid IT environments, rapid CI/CD cycles, open source frameworks and languages such as Apache Struts, Rails, and PHP, web-based applications are complicating the enterprise attack surface with more inherited and developed vulnerabilities, while inviting exploits that are increasingly difficult to prevent.

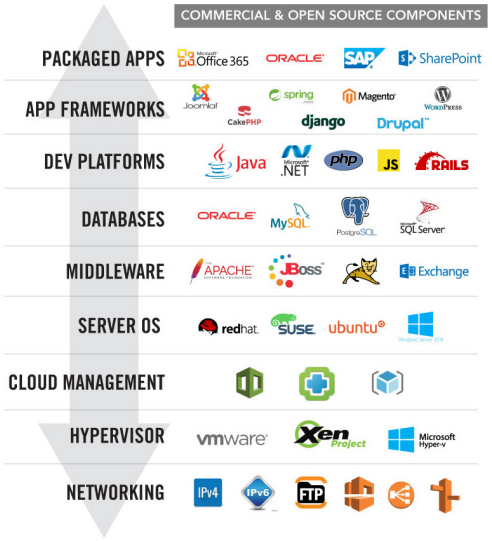
Web application attacks are the #1 attack vector causing data breaches, tripling as a proportion of all breaches from 9.4% to 30% from 2014 - 2017 according to the Verizon 2017 Data Breach Investigations Report.



Web application attacks are the #1 source of breaches.
Source: Verizon DBIR 2017

Alert Logic invests in proprietary research and threat intelligence to understand vulnerabilities, exposures, exploits, methods and attack behaviors at each layer of your application and infrastructure stack and the open source and commercial components within them.

We integrate these unique full-stack insights with other global sources of threat intelligence and content to continually enrich vulnerability and exposure scanning, threat detection analytics, incident reports and blocking logic. The result: vulnerability scans, incident reports and live consultations that give you context and confidence to know when and where to act.



Full-stack security includes continuously updated vulnerability coverage and threat detection logic for all layers of your application and infrastructure stacks.

REBALANCE YOUR DEFENSES FOR CLOUD THREATS

Web applications have long been under-protected. Enterprise spending on network perimeter security has dwarfed application security 23:1[1], yet 59% of IT security professionals said traditional tools work somewhat or not at all in hyper-scale cloud environments[2]. Forcing cloud traffic to pass through perimeter appliances like next-generation firewalls and intrusion prevention appliances creates performance choke points and single points of failure that disrupt business and slow down production applications.

The reflex to block more and more attacks at the perimeter is also increasingly ineffective. Blocking requires ultra-high confidence decisions to be made in milliseconds, but few threats announce themselves so clearly anymore. Those responsible for the most breaches such as SQL injection and cross-site scripting hide in plain sight. They slip past even expensive next-gen firewalls because high-confidence detection requires analysis of multiple data points gathered over time from multiple vectors to confirm.

Alert Logic develops and uses multiple technologies to strike the right balance for cloud and hybrid environments. Web Security Manager Premier, our in-line Web Application Firewall (WAF), targets attacks that follow patterns consistent enough to trigger high-confidence millisecond blocking decisions. A dedicated team in our SOC continuously tunes your blocking and white-listing logic to each of your applications to avoid false positives. The WAF is load-balanced on AWS to support cloud-scale application performance and availability.

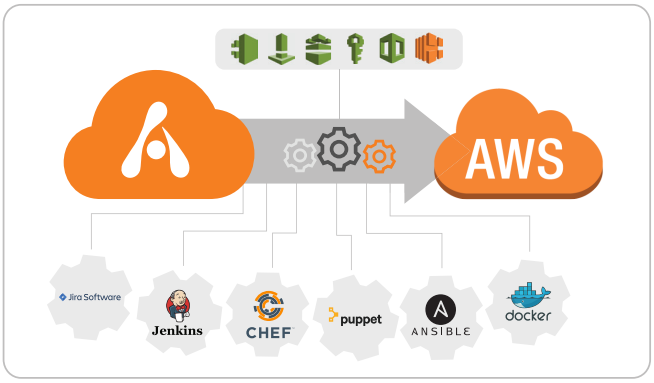
For the remaining majority of attacks, where there is no immediately clear black or white, we use the gold standard in detection: analytics and experts together. Alert Logic ActiveWatch™ - your personal managed detection and response service - uses multiple layers of analytics, including machine learning and anomaly detection as well as signatures and rules. Analytics are used and enhanced by experts from a variety of disciplines including security research, threat intelligence, data science, and Security Operations Center (SOC) analysts. Together, they act as your virtual security team in the cloud, providing 24x365 monitoring, enriched incident reports, remediation advice and live notification within 15 minutes of critical incidents.

*"Partnering with **Alert Logic allows me to keep a leaner team.** Also, instead of drowning in false positives, we only have to wake up at night when there's an actual problem."*
- Wayne Moore, Head of Information Security, Simply Business

ACCELERATE PRODUCTION WITH API-DRIVEN AUTOMATION AND AGILITY

You can see cloud computing's disruptive effect on traditional enterprise security as application, operations and security teams struggle to reconcile opposing security models. The old world: weeks-long, change-controlled, manual releases into IT-controlled data centers guarded by perimeter firewalls. The new world: minutes-long, developer-controlled, automated releases and continuous delivery into cloud platforms where monolithic security gateways inhibit cloud-scale applications.

Alert Logic helps bridge these two worlds with a single workload security solution that uses APIs to integrate into cloud, hosted and on-premises environments. For AWS, Alert Logic has designed security from the ground up for agility and scale. Our microservices architecture and RESTful API are combined with advanced logic that natively understands AWS API outputs, blending security seamlessly into your CI/CD pipeline and dynamic production environment:



- *Buy and pay monthly through AWS Marketplace*
- *Start vulnerability scanning in minutes, expert detection within hours*
- *Scan continuously without manual requests for permission from AWS*
- *Be notified of vulnerabilities throughout your continuous delivery process*
- *Launch and monitor within Docker containers*
- *Adapt security infrastructure automatically as your environment auto-scales*

Visualize impact with dynamic topology mapping

The Alert Logic Cloud Insight service, for example, consumes output from AWS CloudTrail and AWS IAM to continuously discover and model your AWS environment, audit for unsecure configurations, and run agentless scans on software for CVEs (Common Vulnerability Exposures). Most software vulnerability scanning solutions require manual requests from users with root access for permission to perform penetration testing. Pre-authorized by AWS to scan any time, Cloud Insight scans new instances within minutes of being logged by CloudTrail.

In addition to CVE scanning, Alert Logic Cloud Insight performs configuration auditing for AWS environments, alerting you to exposures such as overly permissive security groups or AWS Identity and Access Management (IAM) policies, ELBs using insecure ciphers and Amazon Simple Storage Service (Amazon S3) that allow unauthenticated access.

Configuration exposures and software vulnerabilities are presented in a visual map of your topology helps you explore, understand and see where to take action in your environment. You can pivot by AMI, Instance ID & Type, IP range, Availability Zone, tags and keywords. Grouping instances by AMI shows you the source of the vulnerability, reducing the noise of all the AMI-generated instances with the same vulnerability.

24x365 THREAT MONITORING FOR DOCKER

Containerization has emerged as a popular way for DevOps teams to enable rapid, yet stable, deployment of code changes across all types of production environments. However, it is critical that security teams have visibility to container-level network activity in order to identify potential threats to the environment.

Alert Logic provides security coverage for your containers across numerous deployment models, while also helping you to meet your compliance requirements. Our multi-purpose agent, which is easily added directly into your operating system golden image, binds to **Docker0**, allowing us to capture network activity such as:

- Container-container traffic
- Container-host traffic
- Container-outside world traffic

As a result, we are able to capture all available traffic on the host, which is then processed, analyzed and monitored to ensure your Docker environments are protected.

UNDERSTAND WHY, WHERE AND HOW TO REACT TO AMAZON GUARDDUTY FINDINGS.

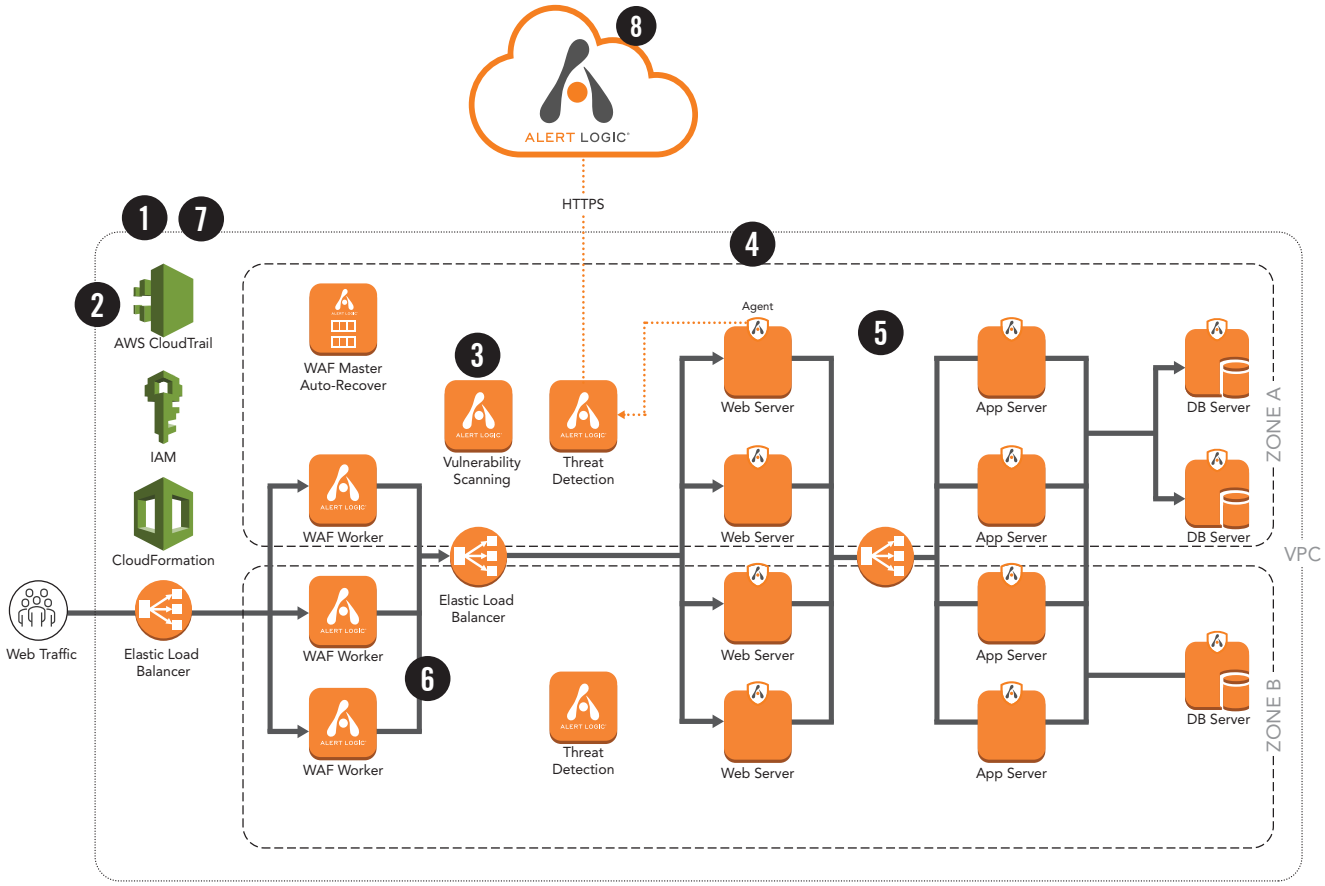
Cloud Insight™ Essentials translates Amazon GuardDuty findings into incidents you can understand, with enriched resource detail and workflow to prioritize and accelerate your responses, including:

- A clear explanation of the Amazon GuardDuty finding
- Added details about affected resources such as tags and VPCs
- Prioritized short- and long-term recommendations to stop active attacks now, and to prevent similar attacks in the future
- Console-based and API-based workflow to initiate, track and resolve incidents

API-DRIVEN SECURITY AS AN AGILE, CLOUD-SCALE SERVICE

One service: Alert Logic Cloud Defender provides an integrated, comprehensive security and compliance solution. Experts Included.

Deploying Alert Logic on AWS is fast and easy. Our software-as-a-service architecture scales to support large migrations and expanding deployments across multiple regions in AWS and on-premises environments.



Conceptual example of a simple 3-tier application

1. **Continuous discovery:** Maintains asset and topology model
2. **Misconfiguration checks:** Identify misconfigurations in accounts and services
3. **Continuous scanning:** Resources and VPCs are scanned within minutes of being created
4. **Continuous detection:** Network and log collectors auto-register as new instances launch
5. **East-West visibility:** Traffic between instances inspected to see lateral movement attack progression
6. **Elastic WAF:** In-line blocking auto-scales to preserve app performance
7. **Continuous compliance:** CloudTrail, IAM logs parsed into standard taxonomy for PCI, HIPAA and SOX reporting, then, stored and searchable for years in our cloud
8. **Offloaded analytics + expert monitoring:** Heavy compute and data storage is done in our cloud with 24x365 monitoring

[1]Gartner Research G00269825, Joseph Feiman, 2014
[2]2016 Cloud Security Spotlight Report, Information Security Linkedin Group Partner, 2016

ALERT LOGIC®