ALERT LOGIC®

iomart

SOLUTION BRIEF:

SECURITY-AS-A-SERVICE
FOR APPLICATIONS IN CLOUD & HYBRID ENVIRONMENTS

Alert Logic solutions combine cloud-based software and innovative analytics with expert services to assess, detect and block threats to applications and other workloads. Protection extends to all layers of your Web application and infrastructure stack to defend against a broad range of server-side threats — including hard-to-detect Web application attacks such as SQL injection, path traversal and cross-site scripting as well as advanced malware, command to control, brute force and many others — while also helping you comply with mandates like PCI, HIPAA and SOX COBIT. Designed for cloud and hybrid environments, Alert Logic solutions use API-driven automation and integration with cloud platforms and DevOps tools.

FULL-STACK SECURITY — Protection across the layers of your app & infra stack

EXPERTS INCLUDED — 24x365 monitoring with live notifications of critical alerts

BUILT FOR THE CLOUD — API-driven automation for cloud and hybrid environments

KEY BENEFITS

With better cloud and Web app protection at a fraction of the total cost and time of traditional security tools, Alert Logic helps you reduce risk while accelerating growth of your business on the Web and in the cloud — without adding security staff.

CLOUD & DEVOPS

- Accelerate production with API-driven security DevOps automation
- Scale and protect with elastic security
- Focus on your business: no security staff or expertise required

APPLICATION OWNERS

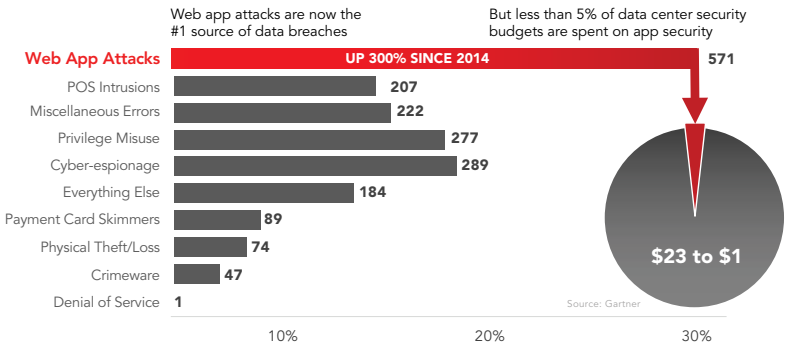
- Innovate safely with security that keeps pace with continuous development
- Prevent attacks by finding vulnerabilities before your adversaries
- Preserve performance and availability with out-of-band detection

SECURITY PRO'S

- Simplify with one service for cloud and on-premises — no new tools to buy
- Expand defenses with accurate, expert protection for your Web apps
- Empower app and cloud pros with agility and protection

OUR UNIQUE APPROACH

Businesses are rapidly becoming more dependent on inherently vulnerable custom Web applications. Accelerated by a potent mix of cloud architectures, DevOps practices, platforms and frameworks such as Wordpress, Magento, PHP and ASP.NET, Web applications are overwhelming traditional enterprise security, expanding the enterprise attack surface with more inherited vulnerabilities and inviting attacks that are increasingly difficult to detect.



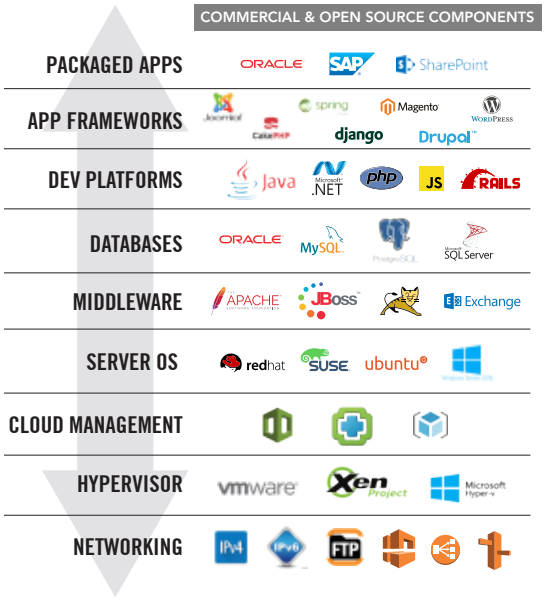
Source: Verizon DBIR 2017

Enterprise investment in network perimeter security has dwarfed application security spending 23:1[i]. But perimeter blocking around DMZs and anti-virus for endpoints are not relevant defenses in the Cloud, nor against Web application attacks like SQL injection and cross-site scripting. 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.

Attackers can use any layer of your application and infrastructure stack, and any third-party component within them, to gain access, build footholds, and laterally move within your system. As the variety and sophistication of exploits continues to explode, even large, mature Fortune 100 security teams are feeling outgunned.

FULL STACK SECURITY

Alert Logic invests in proprietary research and threat intelligence to understand vulnerabilities, exploits, methods and attack behaviors across 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 scanning and threat detection analytics; improve Security Operations Center (SOC) processes for seeing attack progression and verifying severity level. The result: vulnerability scans, incident reports and live consultations that give you confidence and context to know when and where to act.



Full-stack security includes continuously updated insights into vulnerabilities of 3rd party frameworks and libraries

EXPERTS INCLUDED

Security tools alone, particularly when monitoring Web applications, generate mostly false positive alerts that drown out vague true positives. People skilled in Web and cloud threat detection are needed to evaluate machine-generated alerts to see which merit closer scrutiny, then gather context to determine severity and potential courses of action. Unfortunately, there is already a 1M global shortage of skilled security workers today, and it is expected to grow to 1.8M by 2022 .

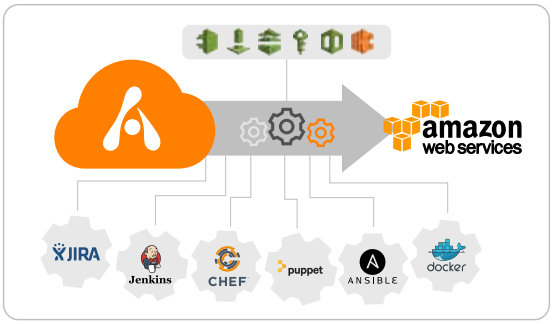
With Alert Logic, experts are "included" as part of an integrated solution with people, process and technology to deliver valuable outcomes such as actionable incident reports and accurate blocking of malicious Web requests. Unlike Managed Security Service Providers (MSSPs) who operate a diverse array of tools their customers buy from different vendors, Alert Logic experts share a common set of tools and processes they help develop and continuously improve, and a multi-petabyte trove of highly consistent data from thousands of customers they use to develop state-of-the-art threat analytics. From Security Operations Center (SOC) analysts and threat intelligence to data scientists and signature developers, Alert Logic has assembled a "dream team" of experts from multiple disciplines so you don't have to. We investigate, research and analyze globally then monitor, enrich, validate and escalate incident reports on your environment so you can stay focused on your business until it's time to act.

*"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*

BUILT FOR CLOUD AND HYBRID ENVIRONMENTS

You can see cloud's disruptive effect on traditional enterprise security as application, operations and security teams struggle to reconcile opposing industry forces. The old world: training, tools and processes designed around weeks-long, change-controlled, manual releases into IT-controlled data centers guarded by perimeter firewalls. The new: minutes-long, developer-controlled, automated releases into cloud service platforms where monolithic security gateways become network chokepoints that inhibit Cloud auto-scaling.

Alert Logic helps bridge these two worlds with a single workload security solution that uses APIs to integrate into both cloud and traditional environments. In any environment, vulnerability scan results integrate with DevOps tools such as Jira and Jenkins while detection agents and virtual appliances can be automatically deployed through a library of templates for Chef, Puppet, Ansible and CloudFormation.



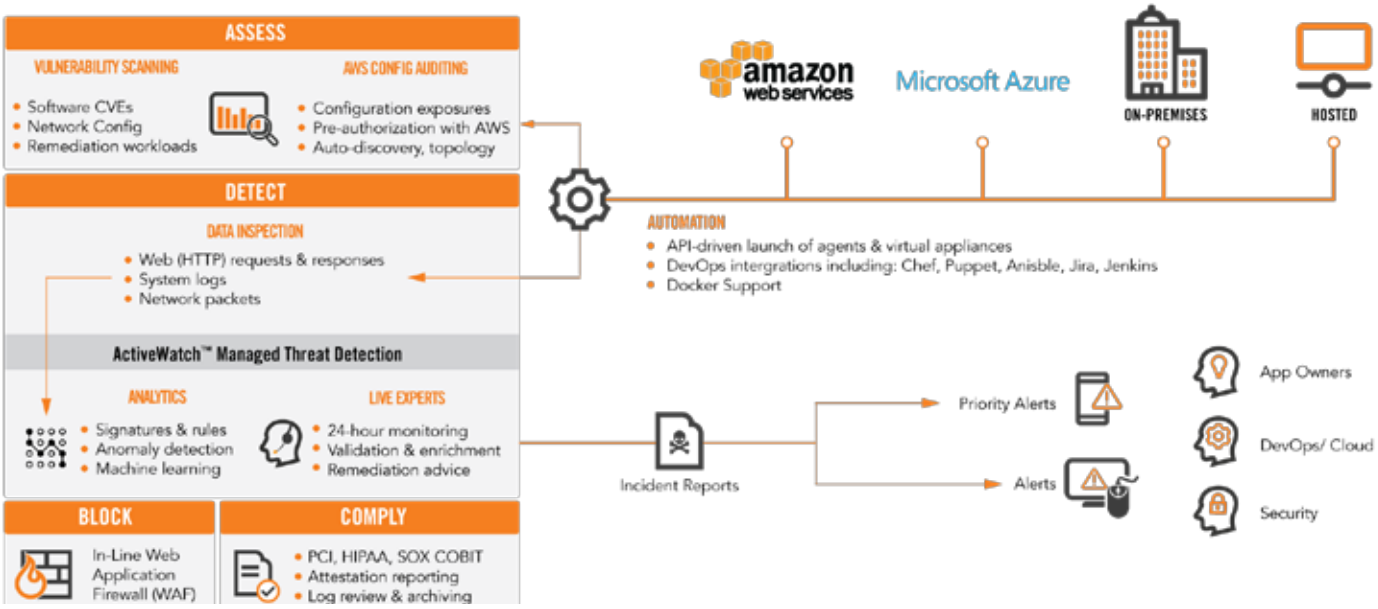
API-driven integration to DevOps and SecOps tools and processes help accelerate production

Taking advantage of Amazon Web Services APIs, Alert Logic adds unique capabilities including agentless software vulnerability scanning, automated configuration vulnerability auditing, auto-discovery and topology mapping and auto-scaling support. Alert Logic is also favored by cloud and application professionals because its out-of-band threat detection doesn't force traffic through chokepoints involving proxies, next-generation firewalls, intrusion prevention systems (IPS) and other forms of appliance-based security gateways, thus preserving performance and availability.

"Alert Logic has a head start in the Cloud, and it shows." *- Forrester 2016 MSSP WAVE™ Report* FORRESTER®

CAPABILITIES

Alert Logic's unique combination of Full-Stack Security, Experts Included and Built for cloud and Hybrid come together into an integrated solution to **ASSESS**, **DETECT** and **BLOCK** threats and help you efficiently **COMPLY** with regulatory requirements.



ASSESS

REDUCE YOUR ATTACK SURFACE BY FINDING VULNERABILITIES BEFORE YOUR ADVERSARIES DO

Vulnerability Management for Common Vulnerabilities and Exposures (CVEs): As application developers increasingly use open source and commercial frameworks and libraries to accelerate their production, they also introduce a long tail of inherited vulnerabilities that increase your attack surface. Alert Logic provides SaaS solutions for DevOps and security teams to run internal, external and PCI vulnerability scans and reports for on-premises, hosted and Cloud environments, with continuous updates to more than 92,000 Common Vulnerabilities and Exposures (CVEs) in software and certain network components.

In AWS environments, CVE scanning is an integral part of Alert Logic Cloud Insight. Cloud Insight consumes APIs including CloudTrail and IAM to run agentless scans. Unlike most solutions that require manual requests for permission to scan, Cloud Insight is pre-authorized by AWS to scan any time. Cloud Insight adapts to your dynamic environment with automatic asset discovery and scanning of new instances within minutes of being added to your environment. Cloud Insight also helps you understand where to take action by maintaining a current visual map of your topology that you can pivot by AMI, Instance ID & Type, IP range, Availability Zone, tags and keywords.

AWS Configuration Auditing: Continuous deployment and uneven experience with AWS best practices increase the risk of launching unknown vulnerabilities in production, including improper configuration of AWS environments and services. 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 IAM policies, ELBs using insecure ciphers and S3 buckets that allow unauthenticated access.

DETECT

ACTIVEWATCH™ MANAGED THREAT DETECTION CUTS THROUGH NOISE FOR YOU 24X365

What we detect: With multiple layers of analytics, security expertise and threat research there is no set limit on which threats we can detect. In addition to common threats affecting workloads including malware, brute force, system level attacks, and privilege escalations, ActiveWatch provides detection of threats specific to Web applications such as

- Exploits against known vulnerabilities in popular Web application frameworks and other app stack components such as WordPress, Magento, PHP, Apache, ASP.Net, MongoDB and Hadoop
- Web application attack methods, including those in the OWASP Top 10 such SQL injection, cross-site scripting, cross-site request forgery, information lead/disclosure, path traversal, code inspection, input validation and authentication issues.

Analytics: Technology and experts are combined to apply three levels of analysis to reduce false positives, improve true positives and provide more context for clear action.

- Signatures & rules: inspecting data for matching one or more criteria, e.g. patterns of exploits against known vulnerabilities or transactions that violate specified parameters
- Anomaly detection: real-time identification of historically unusual behavior, e.g. HTTP requests and responses with characteristics far beyond the normal range previously observed.
- Machine Learning: detection of using algorithms generated and refined by computers under the supervision of data scientists. By finding mathematical patterns too complex for humans to see, machine learning is particularly good at detecting multi-stage, multi-vector attacks that don't match existing signature patterns or anomaly parameters

Data inspection: Data remotely collected by agents and appliances includes network packets, system logs and/or HTTP session requests & responses.

Monitoring: GIAC-certified analysts in our Security Operations Center monitor customer environments globally 24x365. Alerts generated by detection technologies are vetted by analysts to reduce false positives for customers.

Incident Reports: Incidents are enriched by experts with intelligence on the attack type and/or attacker, additional alert and incident correlation, affected resource IDs, suggested actions and other information designed to make your remediation actions more efficient and effective.

Live Notifications: ActiveWatch analysts provide live notification within 15 minutes of high- and critical-priority attacks and can advise the customer on remediation options.

Your ActiveWatch Dream Team

- Threat intelligence analysts look for changes in attack landscape and to understand the latest trends in how adversaries are operating. Alert Logic works with dozens of organizations to gather and share threat intelligence including Recorded Futures, CISP, World Affairs Council and Cloud, hosting and infrastructure partners.
- Security researchers replicate exploits to understand how to better prevent, detect and remediate them.
- Data scientists develop and train algorithms to detect advanced, multi-stage threats
- Security content developers implement new detection and blocking logic such as signatures and rules
- Security Operations Center (SOC) analysts continuously monitor, triage and escalate the most relevant threats to business and application owners

BLOCK

STOP WEB APPLICATION ATTACKS IN REAL-TIME WITH AN EXPERT-MANAGED WEB APPLICATION FIREWALL (WAF)

- Get the active protection of an in-line, proxy-based WAF with negative and positive (whitelisting and blacklisting) models
- Maintain continuity with non-invasive deployment and no application downtime
- Inspect HTTP traffic on day 1 with out-of-the-box rules and signatures covering more than 10,000 vulnerabilities
- Avoid steep costs and learning curves as experts tune blocking rules to the unique characteristics of your Web application
- Support high performance, availability and cost-efficiency by auto-scaling through AWS Elastic Load Balancer
- Quickly meet the WAF requirement of PCI DSS 6.6 while accelerating reporting for PCI, HIPPA and FISMA

COMPLY

IMPLEMENT CONTROLS, ARCHIVE DATA AND AUTOMATE REPORTING FOR PCI, HIPAA AND SOX COBIT

PCI DSS - Achieve compliance and protect card-holder data. Attain compliance with PCI DSS mandates quickly and easily, with guidance from our PCI experts. We provide your quarterly attestation of scan compliance, automate your scanning alerts, reporting and log data archiving. Alert Logic is an Approved Scanning Vendor (PCI ASV Level-2).

HIPAA - Protect sensitive records from attack and comply with healthcare security mandates. Stay vigilant with proactive security alerts and reporting on threats against electronic protected healthcare information (ePHI). Address Meaningful Use Stage One requirements for protection of electronic health information. Alleviate the challenges of addressing audit control requirements with automated security analysis, pre-built alerts, reporting and secure archival with our SSAE 16 Type 2 audited data centers.

SOX COBIT - Simplify and automate the security and reporting mandates for SOX IT compliance controls. Stay up-to-date with proactive alerts on threats and activity that can affect the privacy and integrity of your data. Count on our experts for daily log reviews and 24x365 event and threat monitoring. Eliminate the burden and costs of log-retention and access by using our secure SSAE 16 Type 2 audited data centers.

ALERT LOGIC SECURITY-AS-A-SERVICE OFFERINGS

PACKAGES	ALERT LOGIC CLOUD INSIGHT	ALERT LOGIC THREAT MANAGER™	ALERT LOGIC LOG MANAGER™	ALERT LOGIC WEB SECURITY MANAGER	ALERT LOGIC CLOUD DEFENDER®
EXPERT SERVICES	-	**ALERT LOGIC ACTIVEWATCH™**			
Configuration vulnerability scanning for AWS	●				●
AWS discovery and topology mapping	●				●
AWS software vulnerability scanning	●				●
On-premises vulnerability scanning		●			●
Network data intrusion detection		●			●
Real-time detection analytics		●			●
Detection analytics content subscription		●			●
Expert threat escalation & notification		●			●
Expert threat verification		●			●
Expert live remediation advice		●	●		●
Maintenance of appliance and agent health		●	●		●
Log data inspection			●		●
Log parsing & normalization			●		●
Log retention			●		●
Expert daily log review and alerts			●		●
HTTP request & response inspection				●	●
HTTP response anomaly detection				●	●
Machine learning threat detection					●

DISCRETE SERVICES	
In-line Web Application Firewall (WAF): blocking with ongoing expert services to tune signatures and rules	WEB SECURITY MANAGER PREMIER
Expert log review and preparation for attestation reports for PCI, HIPAA and SOX	LOG REVIEW
Premium Expert Managed Services includes • Named analyst with weekly and quarterly reviews and annual one day on-site • Recommendations on security architecture, policies, processes, configurations • Monitor common stolen data repositories for specific data • Custom signature development and access to custom research	ACTIVEWATCH PREMIER

ALERT LOGIC®

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

- **No Tools to Buy**
  We deliver and manage our own software-as-a-service including analytics
- **No staff to hire**
  Our experts are included
- **No lengthy project**
  Launch security services in minutes
- **No data to integrate and normalize**
  Our data collectors and analytics were designed to work together
- **No content to create**
  We continuously create, deliver and tune signatures, rules and algorithmic detection logic
- **No threat intelligence to Buy and Analyze**
  Threat telemetry and intelligence services are already fully integrated into our detection and escalation services

[i] Gartner Research G00269825, Joseph Feiman, 2014
[ii] Global Information Security Workforce Study, (ISC)2 and Booz Allen Hamilton, Feb. 2017

ALERT LOGIC®