ALERT LOGIC®

SOLUTION BRIEF:

SIEMLESS THREAT MANAGEMENT

SECURITY AND COMPLIANCE COVERAGE FOR APPLICATIONS IN ANY ENVIRONMENT

Evolving threats, expanding compliance risks, and resource constraints require a new approach.

We help organizations who aren't adequately served by other 'solutions' that require installing and configuring security agents, managing data feeds, and wading through alerts. We help organizations who have experienced traditional security outsourcing vendors that fail to deliver little more than yet another alert stream at a high cost. We help organizations left on their own by vendors who provide security products but not threat intelligence or expertise.

Alert Logic seamlessly connects an award-winning security platform, cutting-edge threat intelligence, and expert defenders – to provide the best security and peace of mind for your business 24/7 – at a lower total cost than point solutions, Security Information and Event Management (SIEM) tools, or traditional security outsourcing vendors. We bring a new approach to help you get the right level of security and compliance coverage for your workloads across any environment.

SIEMLESSLY CONNECTED — Platform, intelligence, and experts combined to offer unparalleled threat insights and coverage.

ALWAYS-ON SECURITY — 24/7 monitoring with live notifications of critical alerts.

PROTECTION ACROSS YOUR BUSINESS — Easy-to-use, single-screen view across your cloud, hybrid and on-premises environments.

KEY BENEFITS

We offer a comprehensive managed security and compliance solution at a fraction of the total cost of traditional security tools. Alert Logic helps you reduce risk while accelerating growth of your business — without adding security staff.

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 better security outcomes with agility and protection

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
- Protect application domains with a managed Web Application Firewall (WAF)

TAKE A PROACTIVE APPROACH TO SECURITY AND STAY ONE STEP AHEAD

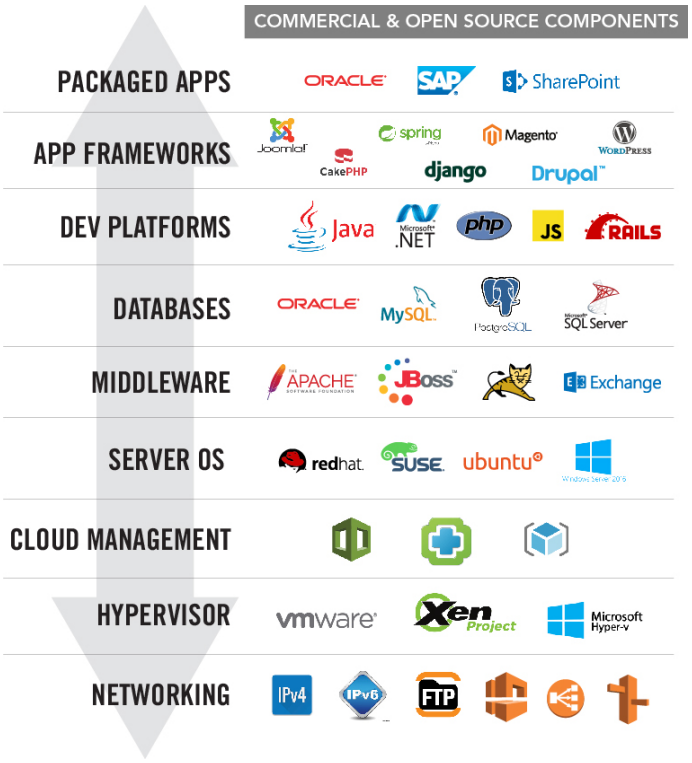
Attackers can use any layer of your application and infrastructure stack, and any third-party component within them, to gain access, build footholds, and laterally move within your system. As the variety and sophistication of exploits continues to explode, even large, mature Fortune 100 security teams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

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 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 access to expertise gives you confidence and context to know when and where to act.

EXPERTS INCLUDED

Security tools alone, particularly when monitoring web applications, generate mostly false positive alerts that drown out 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 1 million global shortage of skilled security workers today, and it is expected to grow to 1.8 million 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 traditional security outsourcing vendors 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.



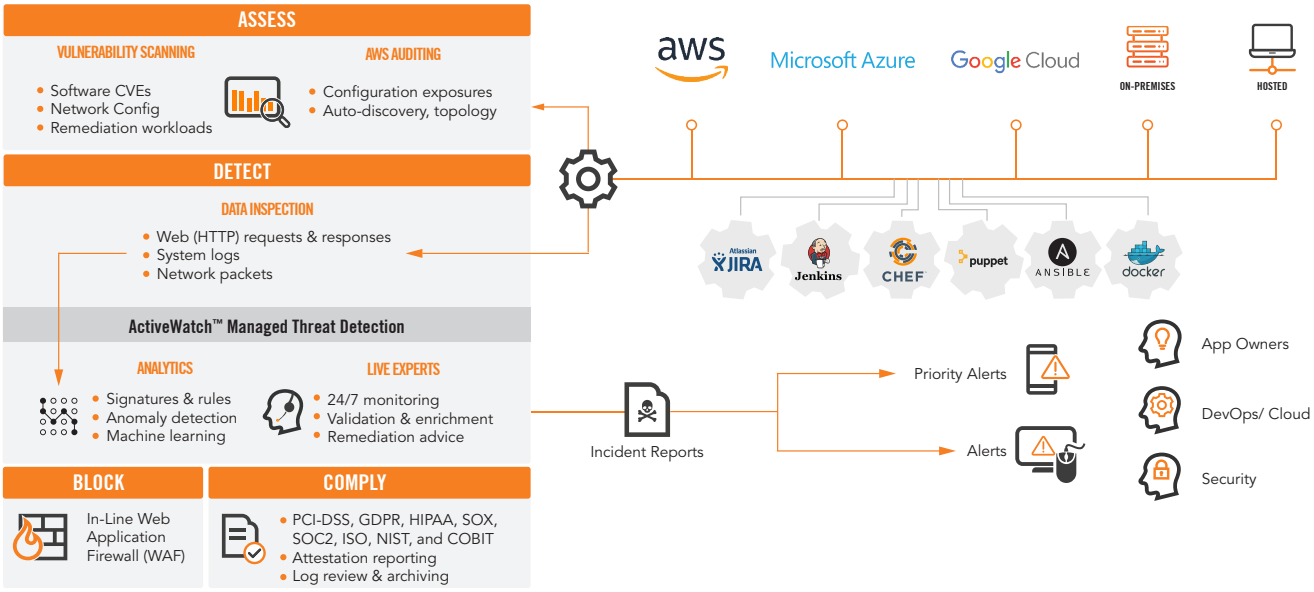
Alert Logic includes platform, intelligence, and experts provide continuously updated insights into vulnerabilities of 3rd party frameworks and libraries

"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

CAPABILITIES

Alert Logic delivers an award-winning security platform, threat intelligence, and expert defenders providing the right coverage for the right resources at a lower total cost. Our solutions seamlessly connect to meet your security and compliance needs.



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 99,000 Common Vulnerabilities and Exposures (CVEs) in software and certain network components.

MANAGED THREAT DETECTION CUTS THROUGH NOISE FOR YOU 24/7

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, Alert Logic provides detection of threats specific to Web applications such as:

- Exploits against known vulnerabilities in popular Web application frameworks and other app stack components
- 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 24/7. 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: Security 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

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

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 daily log reviews and 24/7 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 can assist with scanning, documentation, reporting, and compliance related to PCI-DSS, GDPR, HIPAA, SOX, SOC2, ISO, NIST, and COBIT.

With our SIEMless Threat Management approach, you can easily select the right mix of Essentials, Professional, and Enterprise coverage across your environments. We provide three 24/7 coverage options:

Essentials - Vulnerability and Asset Visibility

Professional - Essentials + Threat Detection and Incident Management

Enterprise - Professional + Managed WAF and Assigned SOC Analyst Options

PRODUCT MATRIX

		ESSENTIALS	PROFESSIONAL	ENTERPRISE
SECURITY PLATFORM The right combination of assessment, detection, and web security technology	Deployment Automation and Scope Selection	●	●	●
	Continuous Asset Discovery and Visibility	●	●	●
	Vulnerability Scanning	●	●	●
	Cloud Configuration Exposure Scanning	●	●	●
	Threat Risk Index	●	●	●
	Security Posture Report	●	●	●
	Comprehensive Reporting Portfolio	●	●+	●++
	Log Management and Search		●	●
	Network Intrusion Detection		●	●
	Log-based Intrusion Detection & Analytics		●	●
	Security Analytics: Rules, Machine Learning		●	●
	Managed Web Application Firewall			Optional
	Web Application Anomaly Detection			Optional
THREAT INTELLIGENCE Up-to-the-minute comprehensive security content and intelligence	Vulnerability and Remediation Content	●	●	●
	Cloud Configuration Exposure Content	●	●	●
	Threat Risk Index Content	●	●	●
	Threat Intelligence Feeds		●	●
	Intrusion Signature Content		●	●
	Log Content		●	●
	Rule Based Content		●	●
	Network Based Machine Learning Content		●	●
EXPERT DEFENDERS 24/7 expert service for deployment, operation, and ongoing security processes	Service Health Monitoring and Support (continuous)	●	●	●
	PCI ASV Support	●	●	●
	24x7 Triage, Escalation and Response Support		●	●
	Security Posture Reviews			●
	Assigned SOC Analyst			Optional
	Threat Hunting			Optional

ALERT LOGIC®