ALERT LOGIC®

ALERT LOGIC® ENTERPRISE

Deeper security coverage for assets, vulnerabilities, and web applications for any environment – with options for an assigned security analyst and managed Web Application Firewall

Business units and IT organizations are struggling to keep up with the current threat landscape. Hiring and retaining staff is difficult and the threats won't stop. Alerts and incidents overwhelm small teams forcing IT to constantly scramble. Building a mature security program requires substantial effort to get to value. Cobbling together a handful of point solutions limits visibility. There is a better way.

With the Alert Logic Enterprise Web Application Firewall (WAF) option, you can block malicious web traffic and reduce false positives. You also get visibility into your environments (cloud, on-premises, or hybrid) and help to identify the remediation steps required to reduce exposures. Our intrusion detection system includes security monitoring and threat analysis from certified security experts with the option of an assigned Security Operations Center (SOC) analyst.

Alert Logic Enterprise provides a deeper connection to our security expertise. Get even greater protection with a managed web application firewall (WAF) protection.

Add an optional assigned security analyst for incident response, security posture reviews, dark web scanning. and threat hunting.

AVAILABLE WITH ALERT LOGIC ENTERPRISE OPTIONS

24/7 Security Operations Center (SOC) Services with an Assigned Security Analyst

- Technical account management
- Security Posture Review
- Escalation support for vulnerabilities
- Threat hunting

Asset and Vulnerability Visibility

- Threat Risk Index
- Server threat visibility
  - Log + Analytics
  - Network IDS

Dark Web Scanning

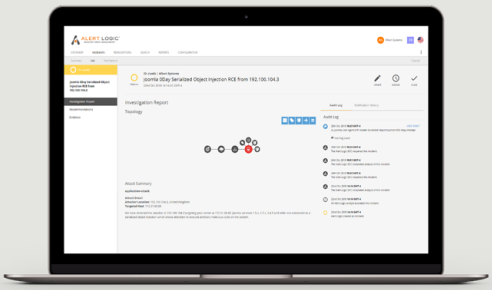
- Proactive scanning and alerting on compromised accounts from your domain(s)

Incident Response Capabilities

- Security experts help in triage, validation and responding to incidents
- Incidents that are enriched with tactical and structural handling recommendations
- Incident interface supports incident investigation and collaboration with Alert Logic analysts
- Supporting services for deployment, 24/7 operations, and security posture review with risk and health improvement recommendations

Access managed WAF protection with curated content and tuning

- Deep web app content and advanced analytics
- Advanced web attack detection content and machine learning models



"Honestly, the attack wouldn't have been something that we would have caught without Alert Logic because we didn't know how to put the patterns together."

Bill Thornton
Vice President, Tango

TANGO

	ALERT LOGIC® ESSENTIALS	ALERT LOGIC® PROFESSIONAL	ALERT LOGIC® ENTERPRISE
	Vulnerability & Asset Visibility with Extended Endpoint Protection	*Essentials* + Threat Detection & Incident Management	*Professional* + Managed WAF & Assigned SOC Analyst options
SECURITY PLATFORM	• Asset discovery • Vulnerability scanning • Extended endpoint protection • Cloud configuration checks • Compliance	• Threat monitoring and visibility • Intrusion detection • Security analytics • Log collection and monitoring • Extensive log search capabilities • Anti-virus and Cloud vendor security integrations	• Always-on WAF defense against web attacks (e.g. OWASP Top 10, emerging threats, zero-day vulnerabilities) • Protection from SQL Injection, DoS attacks, URL tampering, cross-site scripting attacks & more
THREAT INTELLIGENCE	• Threat Risk Index • Remediation guidance • Prioritization and next steps • Comprehensive vulnerability library	• Event insights and analysis • User behavior anomaly detection • Threat frequency, severity, and status intelligence • Attack protection capabilities	• Verified testing against more than 2.1 million web application attacks • Advanced detection capabilities to spot and block malicious activity • Dark Web scanning
EXPERT DEFENDERS	• 24/7 email and phone support • PCI Scanning and ASV support • Service health monitoring	**ACTIVEWATCH PROFESSIONAL** • 24/7 SOC with incident management, escalation, and response support	**ACTIVEWATCH ENTERPRISE** • Security Posture Review • Incident response assistance • Threat hunting • Help with tuning strategies, customized policies, and best practices

ALERT LOGIC®