ALERT LOGIC™

SOLUTION OVERVIEW

Alert Logic MDR Professional

Comprehensive protection for business-critical assets

Addressing threats is a moving target. Monitoring around the clock requires a 24/7 Security Operation Center (SOC), but creating your own can take years. High costs and staffing challenges mean that organizations struggle to identify, prioritize and respond to threats.

Alert Logic MDR Professional protects your business-critical assets with 24/7 threat detection and incident management with a 15-minute triage SLA, MDR Concierge support, vulnerability scanning, asset visibility, and endpoint detection. Our global SOC is staffed by over 150 experts in security and information technology disciplines. They combine the Alert Logic MDR platform and purpose-built SOC tooling with decades of experience.

ALERT LOGIC MDR PROFESSIONAL INCLUDES:

- 24/7 Threat Management
- 15-Minute Escalation SLA
- Named MDR Concierge
- Cloud Change Monitoring
- Real-time Reporting
- Intrusion Detection
- Anti-Virus Integration
- User Behavior Anomaly Detection (UBAD)
- Container Intrusion Detection
- File Integrity Monitoring
- Web Log Analytics

With Alert Logic MDR Professional, You Receive

HYBRID ASSET AND RISK DISCOVERY

The Alert Logic MDR platform has been built to provide a common view on asset vulnerabilities and configurations on all your environments. Through Alert Logic's dashboards, you can rapidly see relevant information that allows targeted response and analysis of those things that affect security posture. In-depth insights into vulnerabilities, attacker behavior, and validated security incidents are just one click away.

EMERGING THREAT RESPONSE

Alert Logic's MDR platform gives our security experts an unparalleled view of attacker behavior across hundreds of thousands of systems. Threat researchers work with this data and intelligence gathered from the security community and industry feeds to identify emerging threats that can affect our customers.

The experts in our security operations center use threat hunting methods to search through massive data sets to identify customers who can be affected by these threats, and alert them to vulnerable systems and work with them to stop attacks before they happen. With hundreds of new vulnerabilities discovered every week, this capability, combined with detection of well-known and established threats, is critical to protect your organization.

MDR CONCIERGE

The MDR Concierge is a single point of contact that is an expert in the delivery of Alert Logic's MDR solution and understands each customer's unique business needs to ensure the best possible service and protection.

	MDR ESSENTIALS	MDR PROFESSIONAL	MDR ENTERPRISE[†]
SERVICE ELEMENTS			
Implementation Support	●	●	●
24/7 Platform Support	●	●	●
Vulnerability Insight Support	●	●	●
PCI Dispute & PCI DSS & ASV Program Support	●	●	●
MDR CONCIERGE		●	●
24/7 Threat Management		●	●
15-minute Escalation SLA		●	●
Emerging Threat Response		●	●
On-Demand Tuning & Sensor Optimization		●	●
Expert Log Review		●	●
DESIGNATED SECURITY EXPERT			●
Continuous Threat Hunting			●
Pro-Active Tuning & Sensor Optimization			●
Extended Security Investigations			●
Weekly Security Review			●
Annual On-site			●
FEATURES			
Hybrid Asset Discovery	●	●	●
Internal & External Vulnerability Scanning	●	●	●
Cloud Configuration Checks/CIS Benchmarks	●	●	●
Endpoint Detection	●	●	●
PCI Scanning	●	●	●
File Integrity Monitoring		●	●
Network Monitoring		●	●
Log Data Monitoring		●	●
Log Collection & Search with 12 Month Retention*		●	●
Web Log Analytics		●	●
Real-time Reporting & Dashboards	●	●	●
Cloud Security Service Integration		●	●
Cloud Change Monitoring		●	●
User Behavior Monitoring		●	●

† Alert Logic MDR Enterprise requires Alert Logic MDR Professional licences for protected assets included in the Alert Logic MDR Enterprise service

* Log retention is always on-line, no restriction on search window exists and more than 12 months retention is available on-request

Contact us to learn more: www.alertlogic.com/mdr

© 2020 Alert Logic, Inc. The information contained in this document is confidential and only for the use of the intended recipient. You may not publish or redistribute this document without advance permission from Alert Logic