ALERT LOGIC™

SOLUTION OVERVIEW

Alert Logic MDR Essentials

Combat your risk of exposure and protect your endpoints

In order to protect an organization, security teams must have visibility into deployed assets, misconfigurations, and vulnerabilities across their entire IT estate.

Alert Logic MDR Essentials provides 24/7 hybrid visibility and vulnerability scanning, audit-ready reporting, and endpoint detection. This allows you to track asset movement and changes, identify exposures that could lead to compromise, and protect client machines using machine learning and behavioral analytics.

ALERT LOGIC MDR ESSENTIALS INCLUDES:

- 24/7 Platform Support
- Hybrid Asset Discovery
- Vulnerability Insight Support
- PCI DSS & ASV Support
- Topology Map
- Cloud Configuration Assessment
- Endpoint Detection
- Real-time Reporting
- CIS Benchmarking

With Alert Logic MDR Essentials, 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.

ENDPOINT DETECTION

Alert Logic's endpoint detection helps thwart multiple attack techniques that try to compromise endpoints, gain access to resources, and detonate payloads, and provides deep visibility in real-time across endpoints, including low-level system activity, without impacting performance.

ESSENTIAL COMPLIANCE COVERAGE

Alert Logic provides complete compliance solutions that give customers peace of mind and deliver on best practices for PCI DSS Compliance, HIPAA HITECH, GDPR, Sarbanes-Oxley (SOX), SOC 2 Compliance, NIST, ISO, COBIT, and other mandates. Cloud industry best practices can be reported on in real time through certified CIS Benchmarking for AWS and Azure; demonstrate improvements and target activities that improve security posture in the cloud.to learn, understand, and advise on what is critical to your business to help guide and prioritize your operations and delivery programs.

	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		●	●
Machine Learning 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