FORTRA

Solution Brief

Alert Logic MDR® Essentials

Combat Your Risk of Exposure and Protect Your Endpoints

To protect an organization, security teams must have visibility into deployed assets, misconfigurations, and vulnerabilities across their entire IT estate. Fortra's 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.

What You Receive with Alert Logic MDR Essentials

Hybrid Asset and Risk Discovery

The Alert Logic MDR platform provides a common view on asset vulnerabilities and configurations in all your environments. Through our dashboards, you quickly view relevant information that allows for 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

Our detection capabilities helps thwart multiple attack techniques that aim to compromise endpoints, gain access to resources, and detonate payloads, as well as provide deep visibility in real-time across endpoints, including low-level system activity, without impacting performance.

Essential Compliance Coverage

Gain peace of mind and deliver on best practices for compliance with PCI DSS, HIPAA, HITECH, GDPR, Sarbanes-Oxley (SOX), SOC 2, NIST, ISO, COBIT, and other mandates through our complete compliance solutions. Report in real time on cloud industry best practices through certified CIS Benchmarking for AWS and Azure as well as 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.

SERVICE INCLUDES

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

For more information, please visit **alertlogic.com**

SERVICE ELEMENTS	MDR ESSENTIALS	MDR PROFESSIONAL	MDR ENTERPRISE †
Implementation	•	•	•
24/7 Platform	•	•	•
Vulnerability	•	•	•
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			•
Proactive Tuning & Sensor Optimization			•
Extended Security Investigations			•
Weekly Security Review			•
Annual Virtual Stakeholders Meeting			•
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 licenses for protected assets included in the Alert Logic MDR Enterprise service

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

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We've created a simpler, stronger, and more straightforward future for our customers. Our trusted experts and best-in-class portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally for cybersecurity that prevails. Learn more at fortra.com.

