Solution Brief

Alert Logic MDR Professional®

Monitoring and addressing threats is a moving target, requiring a 24/7 Security Operation Center (SOC). Creating your own in-house SOC, however, can take years. High costs and staffing challenges means organizations and their internal teams constantly struggle to identify, prioritize, and respond to threats.

Fortra's 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 more than 150 experts in security and information technology disciplines. They combine the Alert Logic MDR platform and purpose-built SOC tooling with decades of experience.

What You Receive with Alert Logic MDR Professional

White-glove Experience

A key aspect of our white-glove approach to security is our dedicated team of experts. The Alert Logic MDR concierge team includes our SOC team, customer success managers, analysts, and threat researchers dedicated to your success. We understand that threats can happen anytime and anywhere, which is why we work around the clock—continuously monitoring and identifying threats to give you peace of mind.

SERVICE SUMMARY

KEY FEATURES

- White-glove Customer Experience
- 24/7 Threat Management
- 15-minute Escalation SLAs
- 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
- Automated Response

Emerging Threat Response

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

Our SOC team uses threat-hunting methods to search through massive data sets to identify customers who may be affected by these threats, alert them to vulnerable systems, and work with them to stop attacks before they happen. With hundreds of new vulnerabilities uncovered every week, this capability, combined with detection of well-known and established threats, is critical to protect your organization.

Alert Logic Intelligent Response™

Alert Logic Intelligent response relieves IT and security departments of repetitive response tasks and minimizes the need for constant administration. Our flexible, scalable, and integrated approach to protect your entire IT estate provides all essential elements through Alert Logic Intelligent Response: multiple user experiences, recognition of risk profiles, broad coverage of sources, advanced detection capabilities, options for levels of automation, the ability to initiate actions, and a growing range of use cases.

For more information, 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		●	●
Container Threat Detection		●	●
Automated Response		●	●
Real-time Reporting & Dashboards		●	●
Cloud Security Service Integration		●	●
Cloud Change Monitoring		●	●
User Behavior Monitoring		●	●
Marketplace-Style Application Registry		●	●

† 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.