FORTRA™

SOLUTION BRIEF (ALERT LOGIC)

Alert Logic MDR Enterprise

Purpose-Built to Protect Your Highest Risk Assets

Finding highly qualified, experienced professionals to join your in-house security team is extremely challenging. Organizations around the world are competing for a limited number of professionals who have the unique combination of technical acumen and soft skills needed to be responsible for your organization's security posture. Businesses that are dependent on only in-house security teams are finding themselves in a quandary as they know they need security expertise to protect their IT estate.

Fortra's Alert Logic MDR Enterprise is a purpose-built solution that protects your highest risk assets without the expense and hassle of finding and keeping cybersecurity experts on your staff.

SERVICE SUMMARY

KEY FEATURES

- Continuous Threat Hunting
- Proactive Tuning and Sensor Optimization
- Extended Security Investigations
- Custom Response Processes
- Weekly Security Review
- Annual Virtual Stakeholders Meeting

What You Receive with Alert Logic MDR Enterprise

Designated Security Expert

Having direct access to a veteran security expert from our Security Operations Center (SOC) provides you a truly customized experience. Focused on your security and business requirements, your designated expert becomes a member of your team to level up your security maturity. In-depth individualized evaluation, security posture reporting, and personalized threat insights enhance the other Alert Logic MDR services for greater insight into data exfiltration and discovery of advanced persistent threats.

Continuous Threat Hunting

Continuous threat hunting proactively identifies and disrupts cyberthreats that target your business. Informed by research and intelligence and based on known attack methods and unusual activity indicators, experts in our SOC work to identify persistent threats.

Network telemetry, logs from security devices, applications, and systems are analyzed using custom methods and purpose-built tools to find indicators that our threat hunters follow to identify threats. They then collect more data to rapidly uncover time-sensitive insights about active threats to reduce dwell time and stop attacks before they start.

Reporting and Consultation

Your assigned security expert performs proactive security reviews to identify incident and threat trends unique to your environment. Tailored reports detail key findings and recommendations, threat trends, and risk analysis. Weekly meetings with IT and security employees in your organization provide the opportunity to learn, understand, and advise on what is critical to your business to help guide and prioritize your operations and delivery programs.

Proactive Tuning and Sensor Optimization

Thanks to their intimate knowledge of your organization, systems, and security controls, your designated security expert acts as an extension of your team, working in the background to configure, tune, and optimize our technologies and processes based on your unique profile and change programs. Through continuous analysis of threat indicators and behavioral data, we identify false positives and events of no relevance to you, which feed into the tuning procedure.

SERVICE ELEMENTS	MDR ESSENTIALS	MDR PROFESSIONAL	MDR ENTERPRISE †
Implementation	●	●	●
24/7 Platform	●	●	●
Vulnerability	●	●	●
PCI Dispute & PCI DSS & ASV Program Support	●	●	●
Customer Success Manager		●	●
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're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.