FORTRA

SOLUTION BRIEF (ALERT LOGIC)

Extended Detection and Response (XDR)

As threat actors become more proficient, sophisticated, and effective, organizations often turn to point-products as a solution. The result is dozens of tools that lack cohesive visibility across an environment, an inability to correlate the disparate data sources to develop actionable insights and, ultimately, not achieving the security outcomes needed to address ever-present threats.

With tightening budgets, security skills shortages, and a focus on improved security posture, it's no surprise security leaders seek more scalable, sustainable, comprehensive, 24/7 detection and response solutions.

Comprehensive Coverage and Visibility

With Fortra Extended Detection and Response (XDR), visibility extends across the entire IT estate including endpoints, networks, and cloud, as well as third-party vendors and sources. This solution combines industry-leading managed detection and response (MDR) with a lightweight Fortra agent uniquely designed to target endpoint telemetry.

The result: A managed XDR solution offering comprehensive coverage and enhanced visibility. This solution empowers better serviceability for security operations teams to gather insights from richer data collection and telemetry sources to improve mean-time-to-detection (MTTD). Our XDR solution's seamless integration with existing tools like EDR and identity management solutions, as well as existing infrastructure, enables organizations to realize continued value from prior investments while fortifying their security strategy, technology, and expertise.

Broad Detection and Response

Effective extended detection and response solutions require broad coverage, centralized analytics, and automation to quickly identify, analyze, correlate, and take action on unwanted activity. Fortra XDR delivers integrated detection capabilities for known and unknown threats, identifying known threats by analyzing thousands of data points, a broad range of telemetry sources, as well as leveraging threat intelligence from the Fortra Threat Brain. Deep analytics, machine and powerful search functions enable analysts to identify unknown and emerging threats. The outcome is actionable guidance to customers to comprehensively remediate to ultimately reduce the potential impact of an attack (reduce dwell time) and prevent reinfection.

SERVICES SUMMARY

KEY FEATURES

- 24/7 threat management and security expertise
- 15-minute escalation SLA (critical and high incidents)
- Security Operations Center (SOC) threat hunting
- SOC-deployed response actions performed for the customer
- Fortra Platform support for Fortra Endpoint Manager
- Automated response (SOAR) for core use cases
- Incident correlation with endpoint and network traffic
- Correlated observations with third-party endpoint and antivirus integrations
- Self-serve, real-time reporting and dashboards on threats, vulnerabilities, topology, and service value

Organizations can gain efficiency with our automated response by streamlining repetitive tasks. This scalable, integrated approach to automation provides the flexibility to take response actions such as host isolation. Our technology is augmented by our SOC team, whereby verified malicious actions detected on the endpoint will result in SOC-deployed response actions on behalf of the customer.

24/7 Managed Expertise and SOC Services

Delivered as a managed solution, Fortra XDR safeguards your business-critical assets with 24/7 threat detection and incident management, delivered by a global SOC team that has extensive experience in security and information technology disciplines. By fusing the Fortra XDR platform technology and a purpose-built SOC tooling with decades of experience, our security operations teams leverage threat intelligence to perform tasks such as incident triage, threat hunting, security investigations, and tuning. Backed by a 15-minute escalation SLA, our managed XDR solution provides continuous monitoring and security expertise giving you peace of mind.

Features and Capabilities

Core features and capabilities delivered by Fortra XDR include:

DETECTION	RESPONSE
• Agent-based scanning • File integrity monitoring • Network traffic inspection • Log collection • OS events, including file, system, host, process, and network activity • File-based attacks (e.g., malware) • Fileless attacks (e.g., PowerShell or registry) • File download and origination • Multi-stage attacks • Threat scoring and prioritization • System scanner and events (user, data, system, command line) • Third-party integrations • Cloud service integrations • Collection of forensic evidence such as web history, event logs, and suspicious files on demand • Utilize MITRE-aligned rules to identify suspicious activity	**Supports third-party and native response actions for:** • Identity management providers • Firewalls • Web application firewalls (WAF) • Endpoint detection and response (EDR) **Response actions:** • Isolate endpoint from network • Disable user credentials • Shun malicious connections • Kill processes* • Server-side detection rules for automatic incident response actions* • On-demand forensic artifact retrieval for immediate incident analysis*

To install the agent, the following server operating systems are required: **Linux** (Debian, Ubuntu, CentOS, Red Hat Enterprise, SUSE, Amazon Linux), **Windows** (Windows Server 2003 SP1 through 2022)

To install the agent, the following client operating systems are required: Windows 10, Windows 11, macOS*

* Targeted for 2024 release

ADDITIONAL FEATURES	XDR
Endpoint Detection & Response	●
Automated Response	●
Log Data & Network Monitoring	●
Log Collection & Search with 12 Month Retention*	●
File Integrity Monitoring	●
Web Log Analytics	●
Machine Learning Log Review	●
Container Threat Detection	●
User Behavior Monitoring	●
Cloud Security Service Integration	●
Cloud Change Monitoring	●
Real-time Reporting & Dashboards	●
Marketplace-Style Application Registry	●
Hybrid Asset Discovery & Inventory	●
Internal & External Vulnerability Scanning	●
Cloud Configuration Checks/CIS Benchmarks	●
PCI Scanning	●
SERVICE ELEMENTS	
Implementation Support	●
24/7 Platform Support	●
Vulnerability Insight Support	●
PCI Dispute & PCI DSS & ASV Program Support	●
XDR Security Value Review	●
24/7 Threat Management	●
15-minute Escalation SLA	●
Emerging Threat Hunting	●
On-Demand Tuning & Sensor Optimization	●
Managed Containment	●

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

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

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.

