FORTRA®

DATASHEET (ALERT LOGIC)

Fortra Extended Detection and Response (XDR) for IBM i Servers

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.

Integrate Your IBM i Logging and XDR

For customers running critical business applications on IBM i, Fortra Extended Detection and Response (XDR) seamlessly ingests and processes log data from the IBM i, enabled by the Powertech SIEM Agent for IBM i. This allows security teams to monitor events from IBM i and other operating systems within one centralized dashboard, reducing the likelihood that a critical IBM i security event goes unnoticed while minimizing IT's workload.

Key Benefits

Comprehensive Coverage and Visibility

Fortra XDR offers complete visibility into all security events spanning an organization's entire IT estate. This includes endpoints, networks, cloud, and third-party vendors and sources. Combined with industry-leading managed detection and response (MDR) and a lightweight Fortra agent uniquely designed to target endpoint telemetry, Fortra XDR makes gathering and acting on security insights as easy and effective as possible.

Centralized Management

Fortra XDR and Powertech SIEM Agent allow cybersecurity and operations teams to host all critical security messages in a centralized location. This eliminates any duplication of detection and response efforts and reduces the likelihood of a threat going unnoticed.

Tool Integrations

Fortra XDR and Powertech SIEM Agent integrate with existing tools like endpoint detection and response, identity management, and IBM i job scheduling

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
- Correlation observations with third-party endpoint and antivirus integrations
- Self-serve, real-time reporting and dashboards on threats, vulnerabilities, topology, and service value.

solutions to multiply the value of your existing investments while fortifying your security strategy, technology, and expertise.

Protection from Known and Unknown Threats

Fortra XDR identifies known threats by leveraging threat intelligence from the Fortra Threat Brain in its analysis of thousands of data points and a broad range of telemetry sources. Deep analytics, machine learning, and powerful search functions enable analysts to identify unknown and emerging threats.

Improve Efficiency and Time to Response

Organizations can gain efficiency with our automated response by streamlining repetitive response tasks 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.

Overcome Staff Shortages with a 24/7 Managed Service

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 with more than 120 experts in security and information technology disciplines.

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, providing you with 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 • Application attacks • Credential attacks • Lateral movement • Command and control communication • 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 • User behavior analysis • Anomaly detection • 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 • Reset user session • Force password reset • Remove MFA devices • Shun malicious connections **Use Cases:** • Block reconnaissance attempts • Block application attacks • Quarantine compromised accounts • Reset compromised accounts • Prevent infection spread • Limit malware and ransomware • Block command and control traffic

To install the agent on Linux or Windows, the following server operating systems are required: Linux (Debian, Ubuntu, CentOS, Red Hat Enterprise, SUSE, Amazon Linux), Windows (Windows Server 2003 SP1 through 2022). A 64-bit Intel/AMD or ARM CPU is required.

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

To install the Powertech SIEM Agent on IBM i (AS400), you will need IBM i OS level 7.3 or higher. We can install on unsupported OS levels too, but please call our support team for special downloads.

SERVICE ELEMENTS	XDR
Implementation	●
24/7 Platform	●
Vulnerability	●
PCI Dispute & PCI DSS & ASV Program Support	●
Customer Success Team	●
24/7 Threat Management	●
15-minute Escalation SLA	●
Emerging Threat Response	●
Structured Threat Hunting	●
On-demand Tuning & Sensor Optimization	●
Machine Learning Log Review	●
Designated Team of Cyber Risk Experts	●
Bespoke Threat Hunting	Available as Add-on
Proactive Tuning & Detection Optimization	Available as Add-on
Security Posture Consultation	Available as Add-on
Tailored Response Playbooks	Available as Add-on
Biweekly Security Review	Available as Add-on
Annual Virtual Stakeholders Meeting	Available as Add-on
FEATURES	**XDR**
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	●
User Change Monitoring	●
Managed Containment	●
Third-Party EDR Integration and Response	●
Single Fortra Agent	●
Fortra Threat Brain Intelligence and Analytics	●
Third-party Network and Identity Response	●
Fortra Platform Support	●
Incident Correlation with Endpoint and Network Traffic	●

* For qualifying customers. Log retention is always online, no resriction on search windows exists, and more than 12 months retentiion is available upon request.

For more information, contact your Fortra account representative.

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.

