FORTRA™

VISUALIZING

Alert Logic MDR

Fortra's Alert Logic Managed Detection and Response (MDR) solution creates cyber resilience at scale with integrated services that discover risks to the security of your business and security operations center (SOC) experts that detect breaches. Alert Logic allows you to better withstand and rapidly respond to cyberattacks.

We assess your security posture and collect data across all your systems to analyze, prioritize, and validate threats before escalating only those that can impact your business — providing vital and actionable intelligence.

Coverage for major platforms and services, including:

aws · Azure · Active Directory · CROWDSTRIKE · okta · SOPHOS

Assess

Alert Logic provides a 360° view of your exposures, combining the findings from agent-based scans, network scans, external scans, and API checks. With this information, you can understand your unique security posture through reporting, dashboards, and expert services.

10k+
Types of Configuration Problems Assessed

205k+
Unique Vulnerabilities Scanned from a Continually Updated Library

Collect

Fortra's Alert Logic MDR monitors ...

>3.3m
Servers, Containers, and Endpoints

140b+
Log Messages per Day

36PB
Log data and network traffic, available in single data lake, for SOC investigations and emerging threat hunting

3.5m
Security Events per Second

Analyze

The **Alert Logic MDR** platform provides a common view of active threats and attacks into all your environments. Incidents are escalated to our SOC experts, who then leverage the platform to investigate and enrich incidents that affect you.

14 **Dashboards:** Daily checks and views-at-a-glance insights into security posture.

31 **Unique Reports:** Enable security and compliance processes through executive reporting.

5k **Unique Log Parsers for Security Detection:** Analyze and monitor the security relevant messages from each log file you send.

46 MONTHLY **Emerging Threat Hunting:** 46 successful threat hunts are escalated to customers each month as part of daily emerging threat hunting.

Prioritize

With Alert Logic, rest easier at night knowing our team is on the job 24/7, escalating only incidents needing your attention, triggering automated response playbooks, and guiding you through the remaining response actions to comprehensively address threats.

450k
Incidents per Month
analyzed through machine learning, advanced analytics, and human validation to eliminate false positives becomes

800
High and Critical Incidents
escalated by SOC analysts

Validate

We're always monitoring so you don't have to. Our team of 150+ SOC and threat intel experts are watching over your environment and identifying compromises before they become an issue:

- Triage, investigate, and enrich with actionable advice
- Reduce noise and false positives
- Trigger response actions with human-validated incidents and context

Alert Logic acts quickly to disrupt threats. Speed is critical when responding to compromise, which is why we commit to a 15-minute SLA for incident triage. On average*, analysts begin investigating within 1 minute of detection, the incident is triaged within 4 minutes, and intelligent response actions initiated within 10 minutes.

~1 MIN*	INVESTIGATE
< 4 MIN*	INCIDENT TRIAGE
< 10 MIN	INITIATE RESPONSE

*Subject to 15-minute SLA

FORTRA™

Detect & Respond with Your MDR Security Ally

REQUEST A DEMO TODAY