FORTRA™
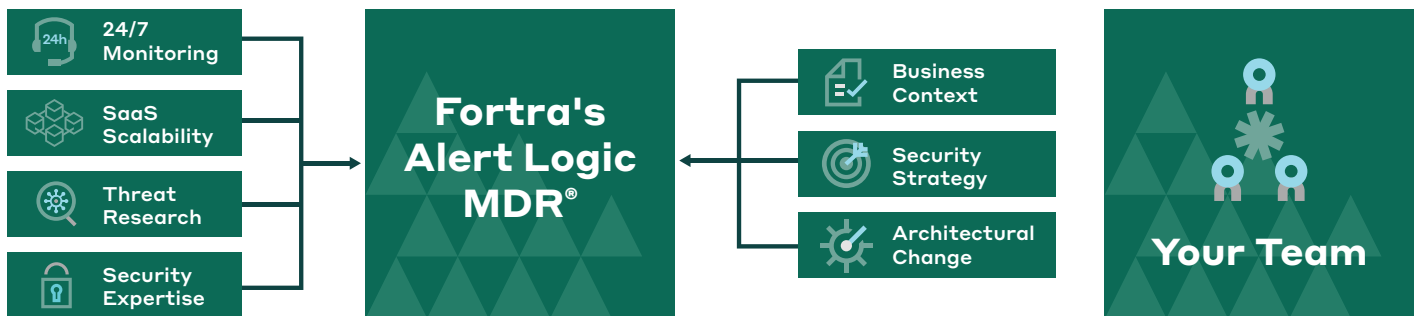
Alert Logic Managed Detection and Response

No Level of Investment Prevents or Blocks 100% of Attacks

As the industry's first managed detection and response (MDR) provider, our purpose-built technology and team of security experts work closely with each customer to understand your unique needs and business context, empowering you to identify and resolve whatever threats, breaches or gaps may come.

24/7 Monitoring		Business Context
SaaS Scalability	Fortra's Alert Logic MDR®	Security Strategy
Threat Research		Architectural Change
Security Expertise		Your Team

Intelligence Driven By Data and Humans

Security experts in our global Security Operations Center (SOC) leverage industry data, continuous research from our threat intelligence team, and machine-learning from aggregated data of thousands of customers. This knowledge provides you vital context about your risk of exposure and exploitation that leads to the most appropriate event response.

Security Insight Always at Your Fingertips

Our platform delivers real-time reporting, giving you access to information on risk, vulnerabilities, remediation activities, configuration exposures, and compliance status. With this intelligence, you can focus on a prioritized order of threats that need further triage, drill down into threats to act on or mitigate exposure, and provide intuitive risk visualization.
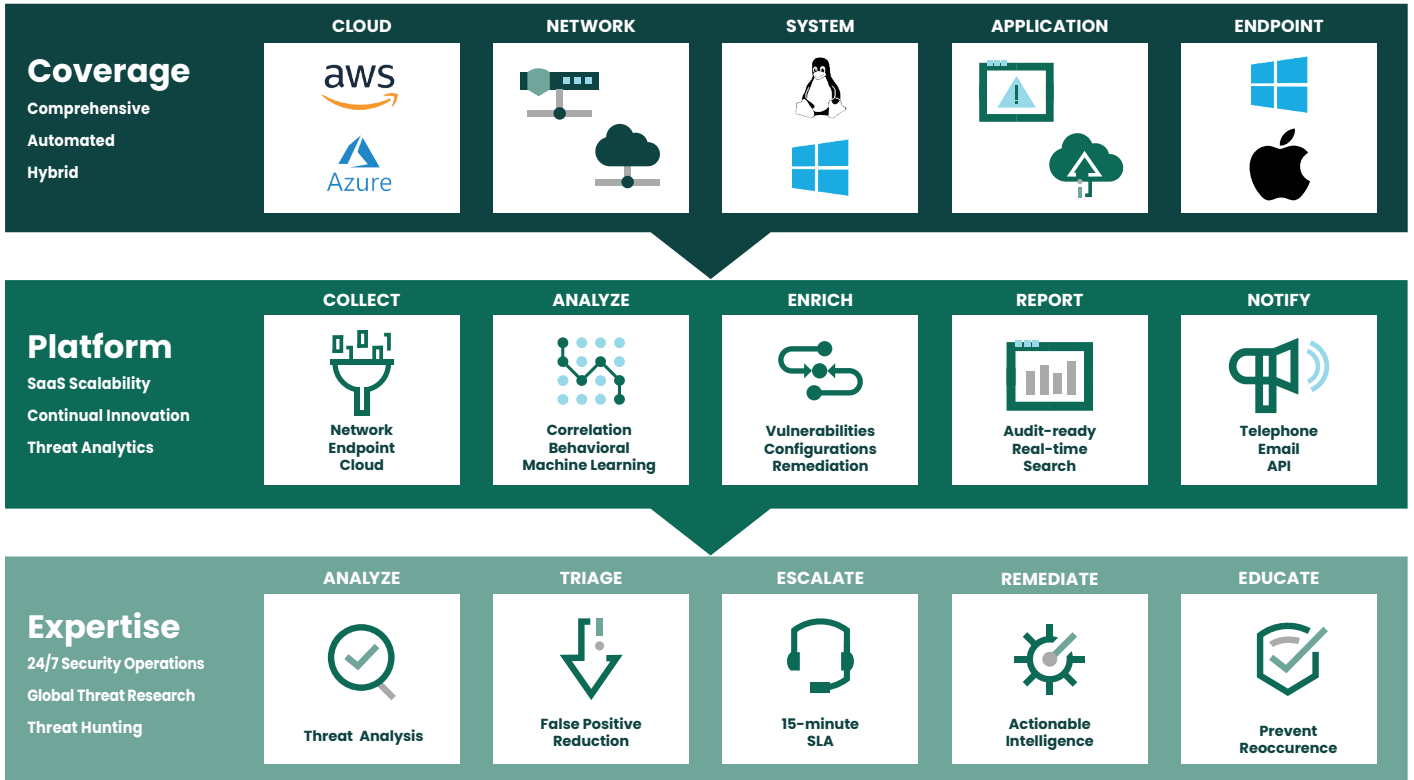
Alert Logic Console Dashboard

Real Security Experts Assigned to Your Account

People are a critical component of Fortra's Alert Logic MDR solution. Each customer is assigned a broad range of security, technology, and customer success professionals who provide a personalized level of service that considers the unique context of your organization.

Scalable MDR Platform

Our proprietary platform analyzes network traffic and more than 140 billion log messages each day. This provides coverage across your entire attack surface and brings together asset visibility and security analytics for cloud, networks, applications, and endpoints in cloud, on-premises, and hybrid environments.

	CLOUD	NETWORK	SYSTEM	APPLICATION	ENDPOINT
Coverage Comprehensive Automated Hybrid	aws / Azure				

	COLLECT	ANALYZE	ENRICH	REPORT	NOTIFY
Platform SaaS Scalability Continual Innovation Threat Analytics	Network Endpoint Cloud	Correlation Behavioral Machine Learning	Vulnerabilities Configurations Remediation	Audit-ready Real-time Search	Telephone Email API

	ANALYZE	TRIAGE	ESCALATE	REMEDIATE	EDUCATE
Expertise 24/7 Security Operations Global Threat Research Threat Hunting	Threat Analysis	False Positive Reduction	15-minute SLA	Actionable Intelligence	Prevent Reoccurence

Tailored Protection to Each Asset in Your Estate

With Alert Logic MDR, you decide on the most appropriate level of protection for each of your assets. This ensures you achieve your desired security outcome with the right coverage at the best possible cost for your business.

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

Our offerings work together across your environments to give you the right coverage with the right resources.

SERVICE ELEMENTS	MDR ESSENTIALS	MDR PROFESSIONAL	MDR ENTERPRISE †
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			●
Proactive Tuning & Detection Optimization			●
Security Posture Consultation			●
Tailored Response Playbooks			●
Biweekly Security Review			●
Annual Virtual Stakeholders Meeting			●
FEATURES	**MDR ESSENTIALS**	**MDR PROFESSIONAL**	**MDR ENTERPRISE †**
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

* For qualifying customers. 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.