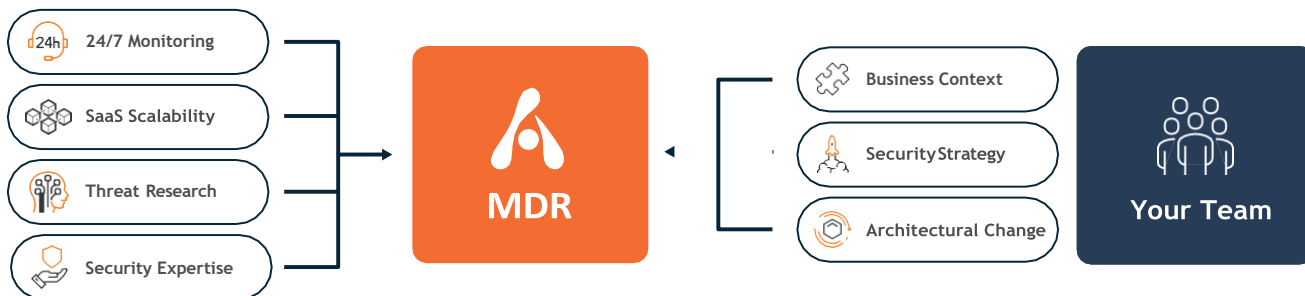# Alert Logic Managed Detection & Response

Protecting your organization and delivering unrivaled security value.

NO LEVEL OF INVESTMENT PREVENTS OR BLOCKS 100% OF ATTACKS

As the industry's first Managed Detection and Response (MDR) provider, Alert Logic's purpose-built technology and our team of security experts work closely with our customers to understand your unique needs and business context, empowering you to resolve whatever threats may come.

24/7 Monitoring
SaaS Scalability
Threat Research
Security Expertise

MDR

Business Context
Security Strategy
Architectural Change

Your Team

INTELLIGENCE DRIVEN BY DATA AND HUMANS

Our knowledge provides the vital context about your risk of exposure and exploitation to enable the most appropriate event response. Industry data, continuous research from our threat intelligence team, and machine-learning from the aggregated data of thousands of customers are leveraged by Alert Logic security experts in our global Security Operations Centers (SOC).

SECURITY INSIGHTS ALWAYS AT YOUR FINGERTIPS

Our platform delivers real-time reporting and provides access to information on risk, vulnerabilities, remediation activities, configuration exposures, and compliance status. We enable you to focus on a prioritized order of threats that need further triage, drill down into threats to act on or mitigate exposure, and provide intuitive visualization of risk.

REAL SECURITY EXPERTS ASSIGNED TO YOUR ACCOUNT

People are a critical component of Alert Logic's MDR solution and we have invested in security talent since 2002. A broad range of security, technology, and customer experience professionals are assigned to each customer, providing a personalized level of service that considers the context of your organization and role.

MDR CONCIERGE

A single point of contact that is an expert in the delivery of Alert Logic's MDR solution and understands each customer's unique business needs to ensure the best possible service and protection.
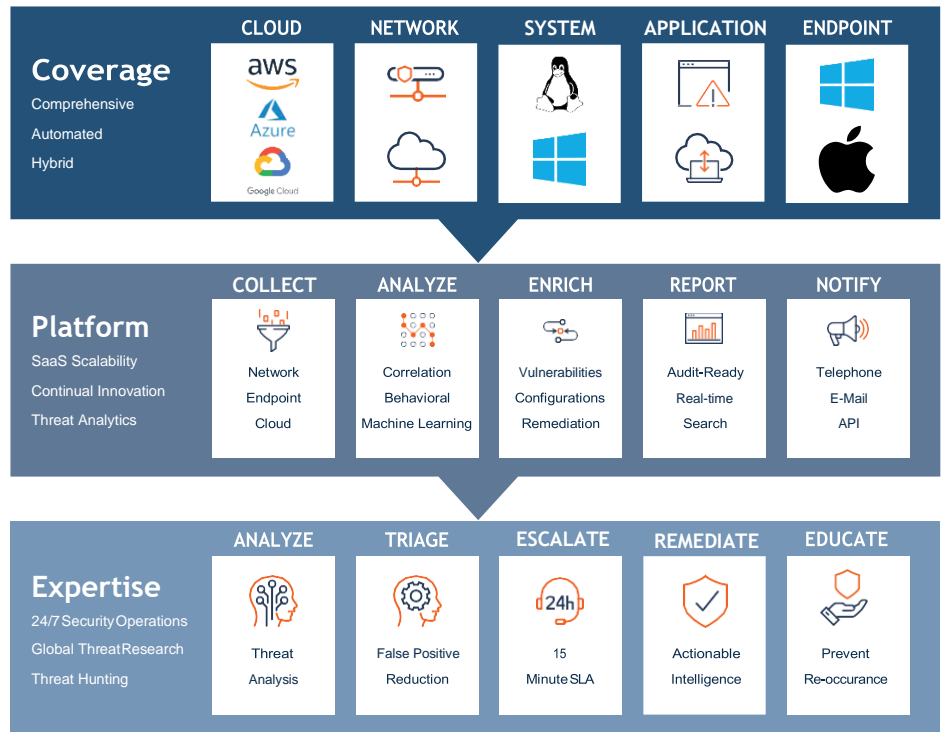
DESIGNATED SECURITY EXPERT

A veteran security analyst in the Alert Logic Security Operations Center (SOC), delivering individualized protection and customized response plans.

Scalable MDR Platform

Alert Logic's proprietary platform analyzes network traffic and more than 60 billion log messages each day, providing coverage across your entire attack surface and bringing together asset visibility and security analytics for cloud, networks, applications, and endpoints in on-premises, hybrid, and cloud environments.

Coverage Comprehensive Automated Hybrid	CLOUD aws Azure Google Cloud	NETWORK	SYSTEM	APPLICATION	ENDPOINT
Platform SaaS Scalability Continual Innovation Threat Analytics	COLLECT Network Endpoint Cloud	ANALYZE Correlation Behavioral Machine Learning	ENRICH Vulnerabilities Configurations Remediation	REPORT Audit-Ready Real-time Search	NOTIFY Telephone E-Mail API
Expertise 24/7 Security Operations Global Threat Research Threat Hunting	ANALYZE Threat Analysis	TRIAGE False Positive Reduction	ESCALATE 24h 15 Minute SLA	REMEDIATE Actionable Intelligence	EDUCATE Prevent Re-occurance

PROTECTION TAILORED TO EACH ASSET IN YOUR ESTATE

We give you the flexibility to choose the most appropriate level of protection for each of your assets to ensure you have the right coverage and achieve the desired security outcome at the best possible cost for your business.

Alert Logic offerings work together across your environments to give you the right coverage, for the right resources.

Service Elements	MDR ESSENTIALS	MDR PROFESSIONAL	MDR ENTERPRISE [†]
Implementation Support	●	●	●
24/7 Platform Support	●	●	●
Vulnerability Insight Support	●	●	●
PCI Dispute & PCI DSS & ASV Program Support	●	●	●
MDR Concierge			
24/7 Threat Management		●	●
15-minute Escalation SLA		●	●
Emerging Threat Response		●	●
On-Demand Tuning & Sensor Optimization		●	●
Expert Log Review		●	●
Designated Security Expert			
Continuous Threat Hunting			●
Pro-Active Tuning & Sensor Optimization			●
Extended Security Investigations			●
Weekly Security Review			●
Annual On-site			●
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 on-line, no restriction on search window exists and more than 12 months retention is available on-request

Contact us to learn more:
https://www.promeromdr.com/contact-us/