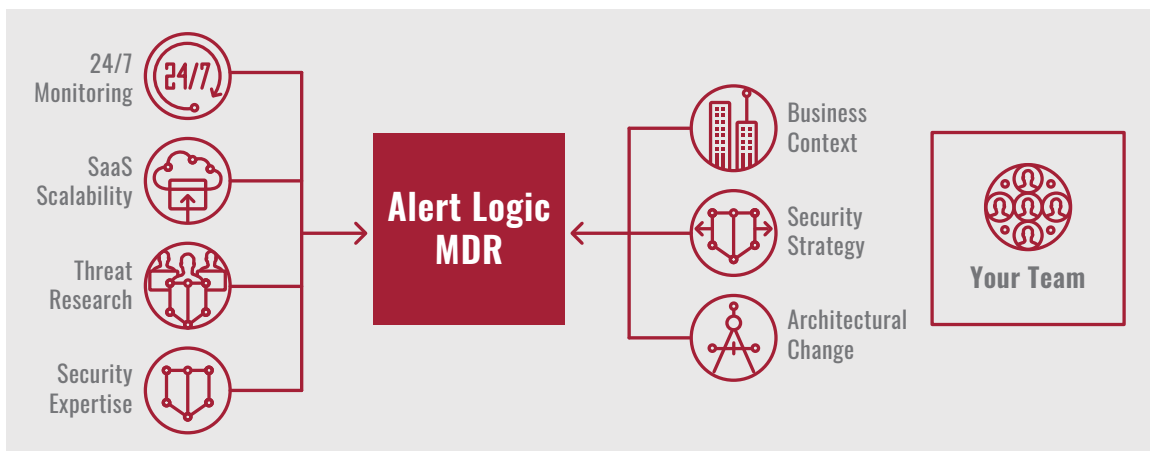# MANAGED DETECTION AND RESPONSE (MDR)

Protect, Detect, Correct.

Managed Detection and Response is a key component of the Aptum Protect portfolio of security services. Aptum is partnering with Alert Logic to deliver industry-leading protection.

NO LEVEL OF INVESTMENT PREVENTS OR BLOCKS 100% OF ATTACKS

Alert Logic MDR is the industry's first Managed Detection and Response offering. Aptum and Alert Logic experts will work closely with you to understand your needs and business context, empowering you to resolve whatever threats may come.

24/7 Monitoring

SaaS Scalability

Threat Research

Security Expertise

Alert Logic MDR

Business Context

Security Strategy

Architectural Change

Your Team

INTELLIGENCE DRIVEN BY DATA AND HUMANS

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

SECURITY INSIGHTS ALWAYS AT YOUR FINGERTIPS

The MDR 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 MDR. 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.
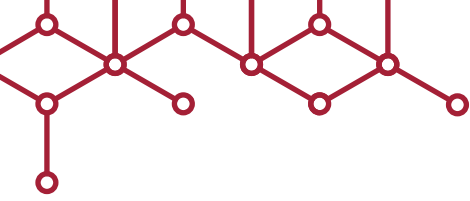
SCALABLE MDR PLATFORM – PROTECTING YOUR ENTIRE IT ESTATE

Our 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

COVERAGE	NETWORK	SYSTEM	APPLICATION	ENDPOINT
aws, Azure, Google Cloud				

PLATFORM

- SaaS Scalability
- Continual Innovation
- Hybrid

COLLECT	ANALYZE	ENRICH	REPORT	NOTIFY
Network Endpoint Cloud	Correlation Behavioral Machine Learning	Vulnerabilities Configurations Remediation	Audit-Ready Real-time Search	Telephone E-Mail API

EXPERTISE

- 24/7 Security Operations
- Global Threat Research
- Threat Hunting

ANALYZE	TRIAGE	ESCALATE	REMEDIATE	EDUCATE
Threat Analysis	False Positive Reduction	15 Minute SLA	Actionable Intelligence	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. Our offerings work together across your environments to give you the right coverage, for the right resources.

	MDR ESSENTIALS	MDR PROFESSIONAL	MDR ENTERPRISE
SERVICE ELEMENTS			
Implementation Support	⊘	⊘	⊘
24/7 Platform 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			⊘
Threat Hunting			⊘
Pro-Active Tuning & Sensor Optimization			⊘
Extended Security Investigations			⊘
Custom Response Processes			⊘
Security Posture Reporting			⊘
Weekly Posture Review			⊘
Annual On-site			⊘
FEATURES			
Hybrid Asset Discovery	⊘	⊘	⊘
Internal & External Vulnerability Scanning	⊘	⊘	⊘
Cloud Configuration Checks/CIS Benchmarks	⊘	⊘	⊘
Endpoint Detection & Response	⊘	⊘	⊘
PCI Scanning	⊘	⊘	⊘
Network Monitoring		⊘	⊘
Log Data Monitoring		⊘	⊘
Log Collection & Search with 12 Month Retention*		⊘	⊘
Real-time Reporting & Dashboards	⊘	⊘	⊘
Cloud Security Service Integration		⊘	⊘
Cloud Change Monitoring		⊘	⊘
User Behavior Monitoring		⊘	⊘

Which Tier Of Alert Logic MDR is for Me?

MDR ESSENTIALS:

MDR Essentials is a self-service model for Alert Logic MDR designed for solutions that are generally low risk to exposure and attacks. The customer is responsible for all aspects of this security tool, so only choose this if you have a good grasp of IT security or have a team that provides that service to your organization. Aptum can provide deployment support but there will be extra charges and fees for this.

MDR PROFESSIONAL:

MDR Professional is the Aptum recommended and preferred tier level of Alert Logic MDR designed for the average solution. It is a fully supported premium white glove experience end to end including onboarding and customization direct from Alert Logic itself. When security is a priority and you want to make sure you are covered, you should take nothing less.

MDR ENTERPRISE:

MDR Enterprise is the highest tier level of Alert Logic MDR that Aptum offers. This includes everything that you get in MDR Professional but you also get the Alert Logic Web Application Firewall and dedicated 24/7 SOC personnel from Alert Logic. If you are running a large company infrastructure and you lack a true Security Operations Center (SOC) then this is the tier that you need. This will bolster security while giving you peace of mind knowing that you are being watched over by one of the most experienced security teams in the world.

No matter the tier you choose, Alert Logic MDR represents one piece of the multi-leveled approach that Aptum takes to protect you and your business that we call Aptum Protect.
Talk to our Sales and Sales Engineers today, so we can help you design a more secure future.

## APTUM REQUIREMENTS FOR MDR CUSTOMERS

SUPPORTED ENVIRONMENTS:

Name	Type
Physical	Colo and Hosting
Virtual	VMware Environments and Aptum Cloud
Public Cloud	Azure

OPERATING SYSTEMS:

Name	Version
Debian	7.x, 8.x
CentOS	7.x, 8.x
RHEL	7.x, 8.x
Windows	2016, 2019

VIRTUAL AND HARDWARE REQUIREMENTS FOR AGENT INSTALLATION:

Components	System Requirements
Memory	96 MB of available memory
Disk space for agent	30 MB of available disk space
Disk space for local cache	500 MB of available disk space
Packet access	WinPcap 4.1.2
CPU Utilization	1-10% depending on log volume
RAM	15 MB minimum
Disk space	30 MB minimum
Log collection support	Windows, Flat File

ALERT LOGIC®
Security. Compliance. Cloud.
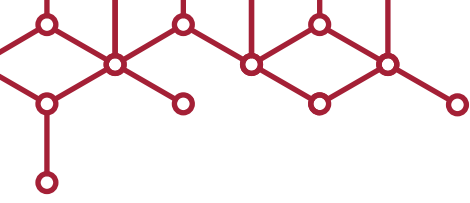
TO LEARN MORE ABOUT HOW OUR SERVICES CAN HELP YOUR ORGANIZATION, PLEASE VISIT:

info@aptum.com
www.aptum.com

ABOUT APTUM TECHNOLOGIES

Aptum Technologies enables customers to unlock the potential of their data infrastructure to drive tangible business outcomes and maximize the value of their technology investments. Aptum's Data Center, Cloud, Hosting and Connectivity solutions, underpinned with expert Managed and Professional Services, offer genuine choice and adaptability combined with international reach spanning North America, Latin America and Europe. In Canada, through its Fiber business, Aptumis the first neutral host provider of turnkey small cell connectivity, augmenting an extensive metro network across Toronto and Montreal. Aptumis a portfolio company of Digital Colony, a global investment firm dedicated to strategic opportunities in digital infrastructure. For more information, visit www.aptum.com.

www.aptum.com

DATA SHEET: MANAGED DETECTION AND RESPONSE (MDR)