CLEARDATA

Managed Detection & Response

Turn Cybersecurity

— INTO YOUR —

Strategic Advantage

The ClearDATA Managed Detection and Response (MDR) service is purpose-built to defend sensitive healthcare workloads and data in the cloud. Our service combines continuous monitoring, threat intelligence, and industry-leading technology to provide a first line of defense against cyber threats and vulnerabilities for healthcare organizations in AWS, Azure, and GCP public cloud platforms.

1 Compliance-Forward Security Innovation

Integrate compliance into every facet of your cybersecurity and gain peace of mind knowing your operations meet the highest compliance standards—such as HIPAA, HITRUST, NIST, and ISO27001.

2 Shared Intelligence & Collaborative Action

Utilize ClearDATA's extensive network to improve the security of healthcare data, enhancing patient information protection, and delivering value by staying ahead of cybersecurity threats.

3 Proactive Threat Mitigation Strategy

Gain crystal-clear visibility and preparative actions to safeguard your sensitive data, so that you have comprehensive threat coverage and rapid threat detection and mitigation.

4 Prioritized Insights, Rapid Responses

Access collaborative and responsive action against threats on your behalf. With our CyberHealth™ Platform, we transform chaos into clarity, equipping you with the tools and guidance to swiftly and confidently tackle cybersecurity challenges while preventing "alert fatigue."

ClearDATA MDR Monitors

Endpoint Threat Protection

ClearDATA's Endpoint Threat Protection offers advanced security for Windows, Linux servers, and container platforms. Managed by their MDR team, it features real-time threat detection and response, protecting against malware, ransomware, and zero-day exploits.

Endpoint Vulnerability Detection

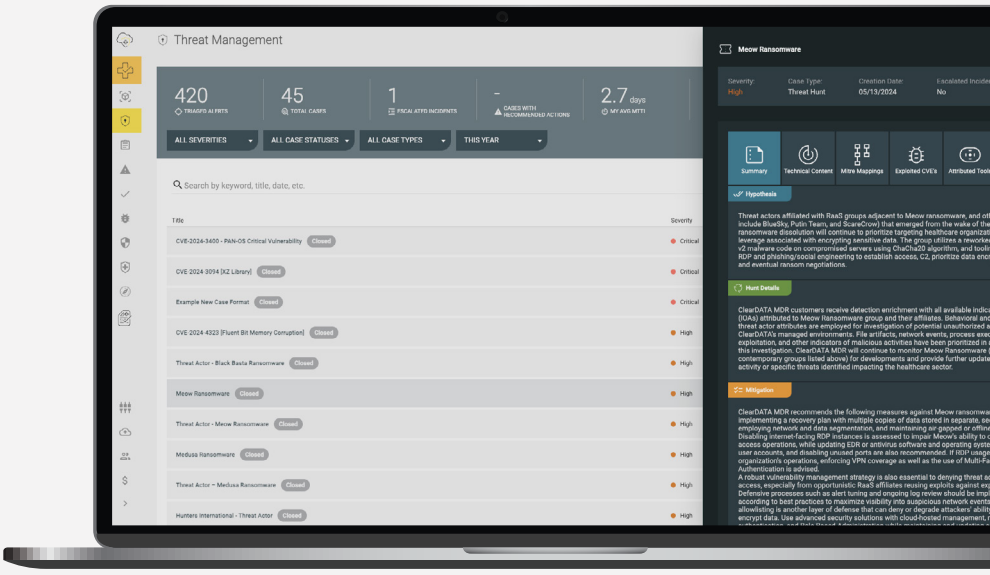
ClearDATA offers a comprehensive Vulnerability Management platform which excels at identifying and reporting software vulnerabilities prevalent in server operating systems and applications.

SIEM & Log Monitoring

ClearDATA MDR analyzes logs with its SIEM platform providing continuos HIPAA compliance and protecting critical system uptime and thereby healthcare access against threats.

Cyber Threat Visibility with the CyberHealth™ Platform

- Gain visibility with interactive dashboards for incident status, exclusive threat intelligence and crucial key performance indicators (KPIs).
- Get real-time status on alerts and actions taken on your behalf.
- Know where to focus with clear-cut intelligence.



Choose Your Level of Protection Suited to Your Business Needs

ClearDATA's highly customizable MDR service — healthcare-specific and based on the NIST Incident Response Framework — ensures you're covered when it comes to potentially devastating cybersecurity threats.

MDR Basics

ClearDATA MDR Basics focuses on the core of threat detection, providing continuous monitoring for irregular activities, streamlined alert triage and investigation to ensure efficient escalation when needed—all tailored to keep your systems secure.

MDR Essentials

ClearDATA delivers robust protection for your infrastructure, networks, and applications through advanced monitoring, detailed logging, and efficient threat containment and removal. By leveraging cutting-edge threat intelligence, it strengthens your overall security posture with precision and reliability.

MDR Complete

The ultimate security package delivers fully customizable protection for your infrastructure, applications, and data. With robust data access monitoring for both cloud storage and databases, this solution ensures your information stays secure. With complete, you can explore customized services and personalized log monitoring to meet your unique needs.

Cyber Threat Protection with Your Best-Fit MDR Solution

Service	Element	MDR Basic	MDR Essentials	MDR Complete
Prepare	Onboarding	✓	✓	✓
	Log & Telemetry Ingestion Planning		✓	✓
	Cloud Configuration & Deployment	✓	✓	✓
	XDR Tuning	✓	✓	✓
Detect & Analyze	Threat Intelligence	✓	✓	✓
	Emerging Threat Notifications	✓	✓	✓
	Threat Hunting	✓	✓	✓
	Threat Detection	✓	✓	✓
	Threat Investigation	✓	✓	✓
	Customer Notification	✓	✓	✓
Respond	Analyst-Initiated Threat Response		✓	✓
Recover	Root Cause Analysis		✓	✓
	Requests for Intelligence			✓
	Remediation Guidance		✓	✓
Report	Regular Reports	✓	✓	✓
	Regular Software Reviews	Annually	Semi-Annually	Quarterly

Alternative Supported Tools and Integrations

With ClearDATA MDR, our security architects and engineers handle the infrastructure, integrations, and event collection, ensuring that telemetry from your cloud environment flows seamlessly into our centralized XDR platform. This empowers you to focus on your core business, confident in the knowledge that your cloud security is being efficiently managed and monitored.

- AWS CloudTrail Management Events
- AWS S3 Object-Level API Activity
- AWS RDS API Activity
- AWS VPC Flows
- AWS Route53 DNS Resolver
- AWS Load Balancer
- AWS Network Firewall
- AWS WAF
- AWS Inspector
- AWS GuardDuty Protection Plan:
  - Foundational Threat Detection
  - S3 Protection
  - EKS Protection
  - Runtime Monitoring
  - Malware Protection for EC2
  - Malware Protection for S3
  - RDS Protection
  - Lambda Protection

- Azure Activity Logs
- Azure Active Directory
- Application Gateway
- Application Gateway - WAF
- Azure Firewall
- Azure Front Door
- Azure Front Door - WAF
- Defender for Databases
- Defender for Containers - Container Runtime Vulnerability Scanning

- GCP Cloud Audit - Admin Activity
- GCP Cloud Audit - Data Activity
- GCP VPC Flows
- GCP Cloud DNS
- GCP Cloud Firewall
- GCP Security Command Center Standard

Windows & Linux Cloud Workloads, Containers and Kubernetes

- Endpoint Threat Protection
- Endpoint Vulnerability Detection
- Server Security Log Monitoring (Auth - Linux)
- Server Security Log Monitoring (Security - Windows)
- Extended Event Collection (File)
- Extended Event Collection (Network)
- Extended Event Collection (Process)
- Extended Event Collection (Registry - Windows)
- Extended Event Collection (Library - Windows)
- Endpoint File Integrity Monitoring

Application Logs

- Apache
- NGINX
- IIS
- HAPROXY
- Windows Application Logs
- Linux Syslog

Container Image Registries

- AWS ECR - Elastic Container Registry
- Azure ACR - Azure Container Registry
- GCP Google Artifact Registry

Reach out today to schedule a consultation with one of our experts, who will help you find the best solution for your organization's healthcare cloud compliance and security needs.

ClearDATA.com (833) 99-CLEAR

Speak with an Expert

CLEARDATA®