MDR for Healthcare

Powered by Google SecOps. Delivered by CloudWave.

MANAGED DETECTION & RESPONSE FOR HEALTHCARE

Modern cyber threats move fast and can outpace detection by traditional defense tools. CloudWave's MDR service, powered by Google SecOps and delivered by healthcare cybersecurity experts, combines advanced detection with human intelligence to hunt, identify, and respond to threats before they can disrupt care delivery or compromise patient data.

PROACTIVE THREAT DEFENSE FOR HEALTHCARE

In today's healthcare environment, attacks can originate from anywhere—phishing emails, compromised remote connections, medical IoT devices, or legacy systems. Reactive defense alone isn't enough. Hospitals need continuous monitoring, proactive threat hunting, and expert-led response to stay ahead of adversaries.

Yet many healthcare organizations face:

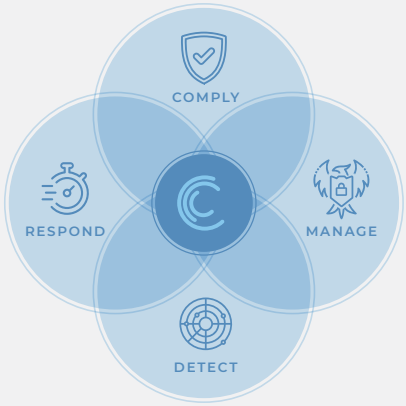
- **Alert fatigue** from disparate tools with no unified response
- **Limited in-house expertise** to hunt for and investigate subtle threats
- **Slow containment** of incidents due to manual processes
- **Compliance pressures** requiring audit-ready reporting and documentation

CloudWave's MDR closes the gap, offering **24/7 SOC monitoring, proactive threat hunting, rapid containment**, and seamless integration with your broader **Managed Security Services** strategy.

24x7 SOC MONITORING

PROACTIVE THREAT HUNTING

RAPID CONTAINMENT



Role of MDR

COMPLY

Demonstrates security controls and reporting to support HIPAA and regulatory compliance

MANAGE

Provides 24/7 SOC oversight and expert threat management

DETECT

Uncovers advanced threats across endpoints, network, and cloud

RESPOND

Delivers rapid containment and guided remediation support

100 Crowley Drive, Marlborough, MA 01752 877-991-1991 **gocloudwave.com**

CloudWave

KEY COMPONENTS & FEATURES

CloudWave Cybersecurity Detection Fabric

- **Security Information and Event Management (SIEM)** – Ingests and correlates logs from CloudWave's Intrusion Detection Toolset and compatible customer assets via Google SecOps
- **Security Orchestration, Automation, and Response (SOAR)** – Automated incident response playbooks for faster containment
- **Intrusion Detection Toolset** – Network and host intrusion detection, deception technologies, and vulnerability management (including a specialized medical device program)

Proactive Threat Hunting

- Human-led investigations to uncover hidden indicators of compromise that automated tools miss
- Integration of Mandiant threat intelligence for faster, more accurate detection

24/7 SOC Monitoring

- Around-the-clock alert triage, threat validation, and remote containment
- Case management system for streamlined collaboration with your security team

Medical Device Cybersecurity Program

- Continuous monitoring and quarterly vulnerability assessments for clinical systems
- Annual device-specific risk assessments and policy templates for medical IoT security

INTEGRATION OPTIONS

- **CloudWave EDR** – SentinelOne-powered endpoint defense integrated with MDR for comprehensive coverage.
- **Advisory Services Bundles** – Add penetration testing, tabletop exercises, or compliance assessments to strengthen your security posture.
- **EHR + Environment Correlation** – Map endpoint, network, and user activity to EHR access for clinical context and PHI protection.

LEARN MORE AT gocloudwave.com

About CloudWave

CloudWave is a leading provider of healthcare cybersecurity and managed services, trusted by over 1,000 hospitals nationwide. By combining industry-leading platforms like Google SecOps with our healthcare-specialized SOC team, we help hospitals proactively defend against threats, protect critical systems and data, respond to incidents, and comply with evolving regulations, ensuring operational resilience and peace of mind.