Managed Security Services

Healthcare-Focused. Patient and Resident-Centered. Expert-Led.

CloudWave's Managed Security Service is a comprehensive, purpose-built solution designed specifically for healthcare, created to help healthcare organizations comply with regulatory requirements, detect threats, and quickly respond to cyberattacks. With 24/7 monitoring, AI-powered threat detection, and specialized healthcare expertise, it delivers end-to-end protection through a single, integrated platform.

COMPLY
Align security with HIPAA, NIST, and HICP

MANAGE
Easy-to-Own, Expertly Handled

DETECT
Data-driven threat detection

RESPOND
Minimize downtime and keep patients safe

A UNIQUELY HOLISTIC CYBERSECURITY STRATEGY

Truly effective cybersecurity in healthcare requires a holistic strategy — one that accounts for connected clinical systems, cloud workloads, and medical devices. That's why CloudWave's Managed Security Service platform is scalable, allowing healthcare organizations of all sizes to comply with cybersecurity best practices and regulations, detect threats or attacks, and respond quickly.

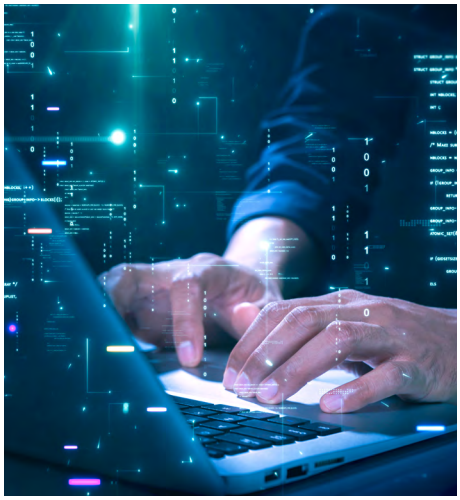
- **Comply:** Align security with HIPAA, NIST, and HICP. Practical solutions to assess your cybersecurity maturity, manage risks, and maintain compliance.
- **Manage:** Easy-to-Own, Expertly Handled. CloudWave's Managed Security Service takes the burden off your internal team by fully managing your cybersecurity program through our 24/7 Security Operations Center. With built-in auto-updates, real-time threat intelligence, and continuous oversight, we ensure your defenses stay current—so you can stay focused on delivering care.
- **Detect:** Data-driven threat detection. Industry-leading tools to help detect threats across your network, endpoints, and medical devices using a multi-layered approach with real-time packet inspection, deception technologies, and monitoring for host-level attacks.
- **Respond:** Minimize downtime and keep patients and residents safe. Quickly contain threats using protocol-driven incident response, automated countermeasures, and support from our 24/7 Security Operations Center (SOC) that will be with you at every step.

COMPLIANCE

CloudWave solutions help healthcare organizations rapidly assess cybersecurity risks, enabling you to prioritize investments, strengthen security posture, and reduce overall business risk.

CloudWave BlueOrange is essentially a managed HIPAA compliance partner — we cover the full lifecycle from initial risk assessment and gap identification through remediation and technical testing to audit readiness and ongoing monitoring.

VULNERABILITY & THREAT MANAGEMENT (VTM)



Comprehensive Risk Visibility Across Your Healthcare Environment

You can't protect what you can't see. CloudWave's Vulnerability and Threat Management (VTM) service gives healthcare organizations continuous visibility across their entire attack surface — from clinical workstations and servers to medical IoT devices and cloud workloads — before attackers find the gaps first.

Why VTM Is Critical for Healthcare

Healthcare environments are uniquely complex. Legacy systems, networked medical devices, and constant regulatory scrutiny create a large and ever-changing attack surface. The result is a set of challenges many teams struggle to fully address:

- Unpatched vulnerabilities on endpoints and medical devices that remain exposed for months
- No unified view of risk across on-premises, cloud, and hybrid environments
- Insufficient resources to prioritize and remediate findings at scale
- Compliance gaps tied to unmanaged vulnerabilities under HIPAA, NIST, and HICP frameworks

CloudWave's VTM service closes these gaps — providing continuous scanning, risk-prioritized remediation guidance, and expert oversight so your team always knows where to act first.

Key Capabilities

- **Continuous Vulnerability Detection:** Active scanning across network assets, endpoints, cloud workloads, and medical devices to identify new vulnerabilities as they emerge.
- **Risk-Prioritized Remediation Guidance:** Vulnerabilities are scored and ranked by exploitability and potential business impact — giving your team a clear, actionable remediation roadmap rather than an unmanageable list of findings.
- **Medical Device Coverage:** Purpose-built visibility into connected medical devices and clinical IoT, including passive scanning methods that avoid disrupting device operation or patient care.
- **Compliance Alignment:** VTM findings and reporting are aligned with industry frameworks (HIPAA, NIST CSF, and HICP), helping support audit readiness and regulatory reporting requirements.
- **Integrated Threat Context:** Vulnerability data is enriched with real-time threat intelligence to highlight which vulnerabilities are being actively exploited in the wild, enabling smarter prioritization.
- **Expert-Led Oversight:** Your VTM program benefits from ongoing security expert analysis and guidance — not just automated reports.

Seamlessly Integrated Within Managed Security Services

VTM works hand-in-hand with CloudWave's broader Managed Security Services platform. Vulnerability data feeds directly into threat detection, incident response, and compliance operations — creating a closed-loop security program where risk is continuously identified, prioritized, and addressed. This integrated approach eliminates the blind spots that siloed point tools leave behind.

Vulnerability data feeds directly into threat detection, incident response, and compliance operations – creating a closed-loop security program where risk is continuously identified, prioritized, and addressed.

MDR FOR HEALTHCARE

Powered by Google SecOps. Delivered by CloudWave.

Google SecOps

Managed Detection & Response for Healthcare

Modern cyber threats evolve rapidly and often evade traditional security defenses. CloudWave's MDR service, powered by Google SecOps and delivered by healthcare cybersecurity experts, combines advanced threat detection, continuous monitoring, and threat hunting to identify and contain threats before they can disrupt care delivery, impact operations, or compromise sensitive patient and resident data.

Proactive Threat Defense for Healthcare

In today's healthcare environment, cyberattacks can originate from anywhere — phishing emails, compromised remote connections, medical IoT devices, third-party integrations, or legacy systems. Reactive defense alone isn't enough. Healthcare organizations 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 proactively investigate advanced threats hunt for and investigate subtle threats
- **Delayed incident containment** due to manual workflows and fragmented processes
- **Compliance pressures** requiring audit-ready reporting and documentation

CloudWave's MDR service closes the gap by providing 24/7 SOC monitoring, identifying threats before they impact organizations, rapid containment, and seamless integration with your broader Managed Security Services strategy.

MANAGED EDR FOR HEALTHCARE

Built on SentinelOne. Powered by Cloudwave.

SentinelOne

Managed Endpoint Detection & Response for Healthcare

Modern cyber threats don't wait — and neither can your response. CloudWave's Managed EDR service — built on the proven SentinelOne platform and delivered by our healthcare cybersecurity experts — helps healthcare organizations detect, contain, and eliminate endpoint threats before they cause harm.

Why It Matters: A Strategic Risk Defense Layer for Healthcare

Endpoints remain the most targeted attack surface in today's healthcare threat landscape. As healthcare organizations expand remote access capabilities, deploy connected medical IoT devices, and adopt cloud-based workflows, the number of vulnerable endpoints — and opportunities for attackers — continues to grow.

Yet many organizations struggle with:

- Alert fatigue from high volumes of noisy EDR notifications
- Limited in-house security resources to investigate, triage, and respond
- Fragmented endpoint protection strategies that leave gaps in visibility or response
- Reactive security operations that struggle to keep pace with evolving threats

CloudWave's Managed EDR, powered by SentinelOne, closes these gaps — offering 24/7 endpoint monitoring, expert-led investigation and response, and seamless integration with your broader cybersecurity posture.

ABOUT CLOUDWAVE

CloudWave is a full-service cybersecurity and cloud services provider exclusively for healthcare. Protecting over 300 healthcare organizations and health systems, CloudWave delivers end-to-end solutions combining secure hosting, IT operations, and 24/7 threat detection. Services include managed security, risk and compliance, disaster recovery, and cloud optimization — all with a healthcare-first approach. Powered by AI-driven security operations and supported by U.S.-based Network and Cybersecurity Tactical Operations Center, CloudWave provides healthcare organizations with a cyber-ready foundation for safe, uninterrupted patient and resident care.