EDR Essentials Guide for Healthcare

CloudWave

Healthcare organizations are under constant siege from cyberattacks. From ransomware campaigns that lock down clinical operations to phishing attacks targeting staff, adversaries see endpoints—laptops, servers, and even medical devices—as the easiest way into a healthcare organization's network.

That's why Endpoint Detection and Response (EDR) has become essential. EDR is more than traditional antivirus—it provides continuous monitoring, intelligent detection, and rapid response to advanced threats. For healthcare leaders, it's a critical layer of defense that protects PHI data, ensures compliance, and helps maintain clinical continuity.

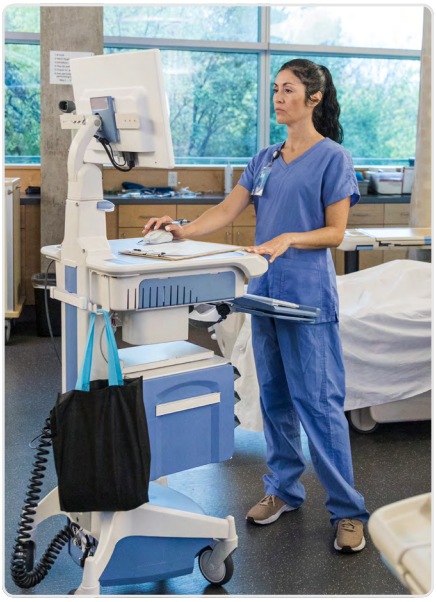
WHY EDR IS IMPORTANT IN HEALTHCARE

The healthcare sector remains the number one target for ransomware, and attackers are becoming increasingly sophisticated. Endpoints are often the first point of compromise, whether through an infected email attachment, a malicious USB drive, or a vulnerable medical device.

Without advanced endpoint security, healthcare organizations face potential:

- **Operational disruption** from downtime or locked systems.
- **Patient and resident safety risks** if devices or EHRs are unavailable.
- **Regulatory consequences** tied to HIPAA and cybersecurity compliance.
- **Financial losses** from incident recovery, fines, and reputational harm.

EDR changes the equation by moving from a reactive posture to a proactive one, detecting suspicious behavior early, containing threats before they spread, and providing clear visibility into how an attack occurred.



WHAT EFFECTIVE EDR DELIVERS

An effective EDR platform provides several core capabilities that traditional endpoint security cannot match:

- **Continuous monitoring** – Always-on visibility across all endpoints, from workstations to specialized medical equipment.
- **AI-driven threat detection** – Machine learning models trained to spot known and unknown malware, fileless attacks, and zero-day exploits.
- **Automated response and containment** – Isolating compromised endpoints within seconds to prevent lateral spread and protect clinical workflows.
- **Forensics and investigation tools** – Providing a detailed timeline of attack activity to aid remediation and strengthen defenses.
- **Integration with SOC/MDR services** – Extending protection with around-the-clock monitoring and expert oversight.

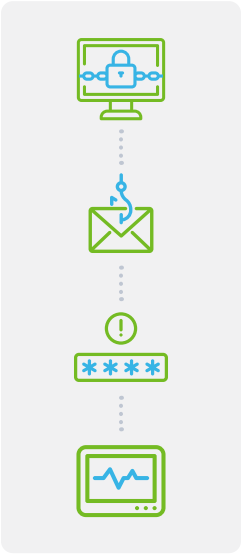
For healthcare organizations with limited internal security staff, the ability to pair technology with managed services is especially valuable.

EDR IN ACTION: COMMON HEALTHCARE USE CASES

EDR provides measurable value in real-world healthcare settings. Here are a few common use cases:

- **Ransomware containment** – Detecting and isolating an endpoint within seconds when malicious encryption activity begins.
- **Phishing attack defense** – Identifying and stopping payloads delivered through phishing emails before they can execute.
- **Insider threat monitoring** – Catching unusual access behaviors that may indicate malicious insiders or compromised accounts.
- **Medical device protection** – Extending protection to connected devices that lack built-in security, reducing the risk of patient and resident-impacting downtime.

These scenarios illustrate how EDR not only stops attacks but also supports compliance and patient and resident safety initiatives.



HOW TO EVALUATE AN EDR SOLUTION

Not all EDR platforms are created equal. Healthcare leaders should look for solutions that are both powerful and healthcare-ready. Key questions to ask include:

- **Does it leverage AI and machine learning** to detect zero-day threats?
- **Can it automatically quarantine endpoints** without disrupting clinical care?
- **Does it account for alert fatigue and false positives** in a healthcare setting, where premature isolation could disrupt patient and resident care?
- **Is it built with healthcare compliance in mind,** supporting HIPAA, HICP, and other frameworks?
- **Does it integrate with your broader security ecosystem,** including MDR, SOC, and SIEM platforms?
- **Is the solution backed by expert support** that understands the context of healthcare workflows?

The answers to these questions will reveal whether an EDR platform is a point product or a true enterprise-grade healthcare defense solution.

SentinelOne

CLOUDWAVE'S MANAGED EDR ADVANTAGE

CloudWave's Managed EDR for Healthcare, powered by SentinelOne, delivers advanced endpoint protection designed specifically for the challenges of healthcare organization and health system environments.

With CloudWave, healthcare organizations get:

- **Technology plus expertise** – Combining SentinelOne's industry-leading EDR with CloudWave's healthcare-focused Security Operations Center.
- **Rapid detection and containment** – Stopping ransomware, phishing payloads, and insider threats before they cause disruption.
- **Healthcare context awareness** – Avoiding unnecessary disruptions to clinical workflows by filtering out false positives.
- **Regulatory alignment** – Supporting HIPAA and HICP cybersecurity best practices.
- **Reduced burden on IT teams** – Providing managed oversight and expert guidance so internal teams can focus on patient and resident care.

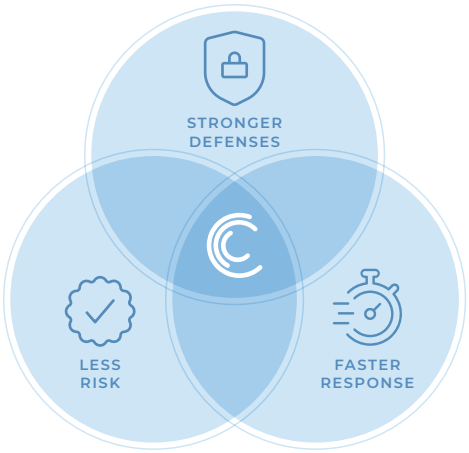
This approach transforms EDR from a standalone tool into a managed service that delivers real protection and peace of mind.

Protecting the endpoint is no longer optional—EDR has become a must-have defense against modern threats.

EDR PROVIDES ESSENTIAL PROTECTION FOR HEALTHCARE

For healthcare organizations, the stakes couldn't be higher. Patient and resident trust, regulatory compliance, and even clinical safety all depend on resilient cybersecurity. Protecting the endpoint is no longer optional—EDR has become a must-have defense against modern threats.

With CloudWave's Managed EDR for Healthcare, healthcare organizations gain a partner that understands both the technology and the unique challenges of healthcare. The result: stronger defenses, faster response, and less risk.



Learn more about CloudWave Managed EDR for Healthcare or request a demo.

MANAGED EDR FOR HEALTHCARE →

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

CloudWave