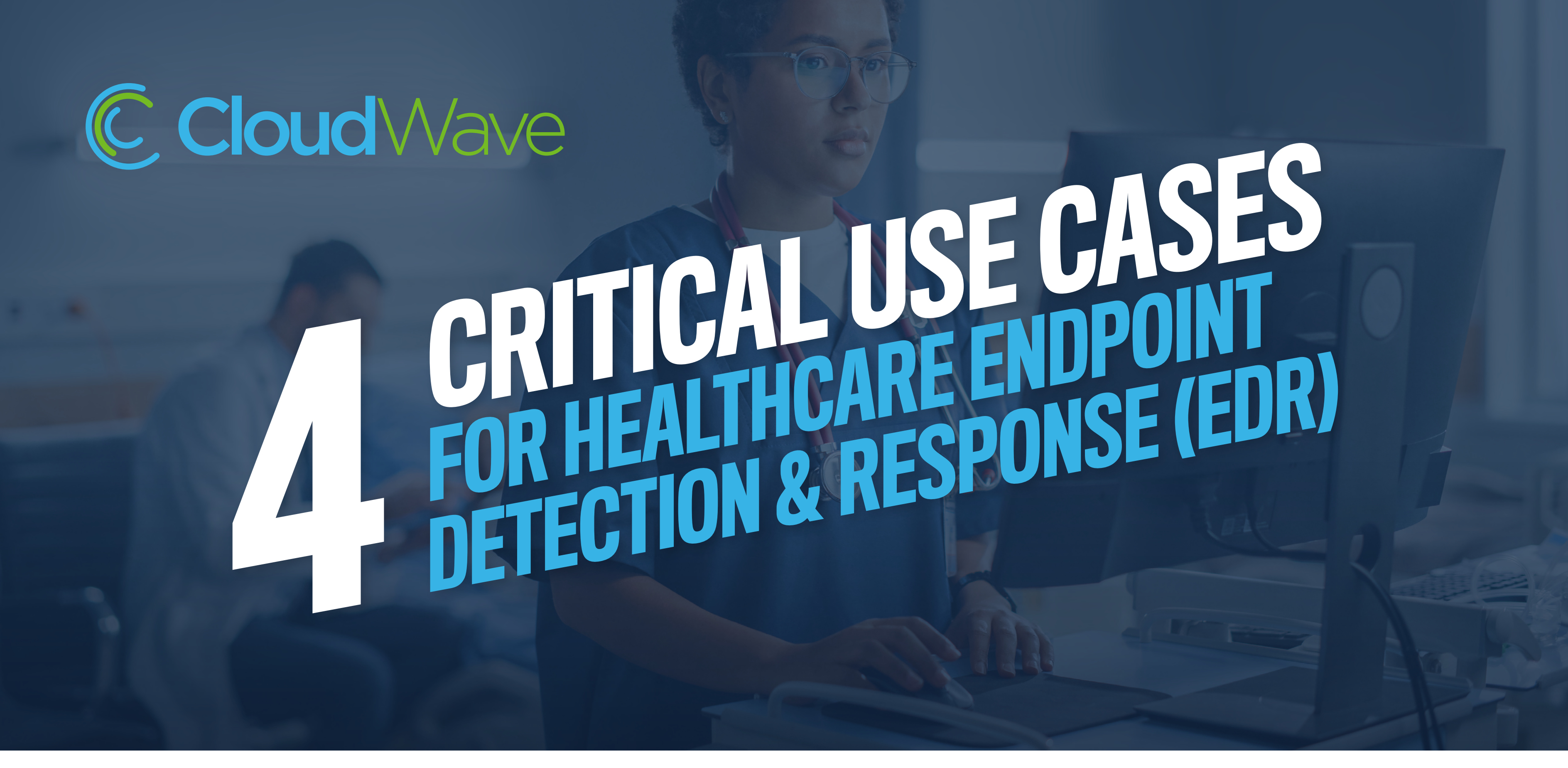
CloudWave



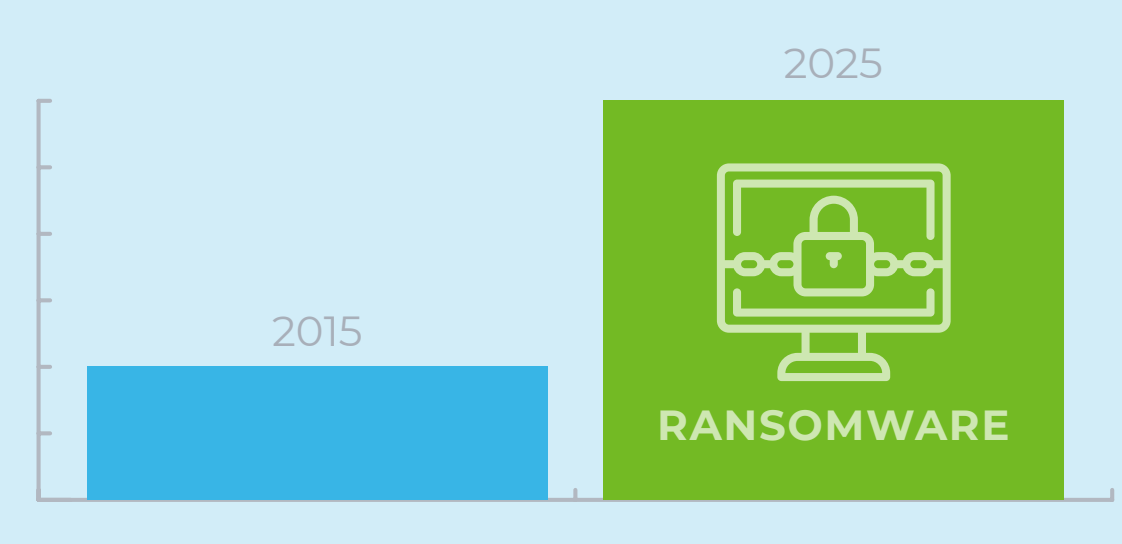
4 CRITICAL USE CASES FOR HEALTHCARE ENDPOINT DETECTION & RESPONSE (EDR)

Threat actors are increasingly exploiting the critical nature of patient care and the complexity of hospital IT environments. **Ransomware, phishing, and advanced persistent threats continue to rise**, as healthcare organizations face the dual challenge of protecting sensitive data while ensuring uninterrupted clinical operations.

Every device, from EHR-connected workstations to mobile tablets used in patient rooms, can be a potential entry point for attackers. As this attack surface expands, traditional perimeter-based defenses are no longer enough.

Endpoint Detection and Response (EDR) has become a crucial component of modern healthcare cybersecurity strategies.

1 STOPPING RANSOMWARE BEFORE IT DISRUPTS PATIENT CARE



+300%

There has been a 300% increase in healthcare **ransomware attacks** in the past 10 years.[1]

The disruption to healthcare operations caused by a ransomware attack can **severely impact the ability to effectively treat patients**—not only at affected hospitals, but also at those in nearby areas.[2]

CHALLENGE

- Ransomware is the **top cyber threat** in healthcare.
- Downtime can delay surgeries, disrupt emergency care, and even **put lives at risk**.
- Traditional antivirus and firewalls **can't keep up** with ransomware's speed or sophistication.

SOLUTION

CloudWave's Managed EDR uses **AI-driven threat detection to identify suspicious activity in real time**, automatically isolate infected devices, and stop lateral spread before systems are encrypted. Our SOC team provides 24x7 monitoring and response expertise to contain incidents immediately.

24x7 MONITORING & RESPONSE

2 PROTECTING CLINICAL DEVICES AND EHR ACCESS POINTS

A typical U.S. hospital has between **10 and 15 medical devices per bed**.[3]

96%

96% of hospitals reported running end-of-life operating systems or software **with known vulnerabilities**.[4]

CHALLENGE

- **Hospitals manage thousands of devices**, from workstations and tablets to imaging machines and medication carts.
- Many of these run **outdated operating systems** or cannot be patched easily, leaving dangerous blind spots.
- Each **unprotected endpoint** creates a **pathway into PHI** and the hospital network.

SOLUTION

CloudWave's Managed EDR **extends protection across ALL ENDPOINTS, even unmanaged or legacy systems**. By delivering real-time monitoring and threat detection across the clinical environment, hospitals gain visibility into every access point that touches patient data.

3 SIMPLIFYING HIPAA & CYBERSECURITY COMPLIANCE

73%

73% of healthcare organizations report **difficulty maintaining comprehensive, audit-ready documentation** of their cybersecurity programs.[5]

STRETCHED THIN

A survey of compliance, risk, and legal leaders at U.S.-based healthcare organizations revealed that a majority of the respondents felt stretched thin **due to the current complex regulatory landscape and expanding areas of risk**, including increasingly sophisticated cyberattacks.[6]

CHALLENGE

- Healthcare organizations must demonstrate to **auditors and regulators** that they have strong endpoint security, continuous monitoring, and documented response capabilities.
- Meeting HIPAA, HITECH, and new HHS Cybersecurity Performance Goals can **overwhelm healthcare IT teams** already stretched thin.

SOLUTION

CloudWave's Managed EDR provides **continuous monitoring, detailed logging, and automated reporting** aligned to compliance standards. Incident response actions are tracked and documented, **creating an auditable trail** that simplifies regulatory reporting.

4 EXTENDING LIMITED SECURITY TEAMS WITH 24X7 COVERAGE

LIMITED BUDGETS

A significant challenge is the limited budgets and resources **for cybersecurity across the healthcare sector**.[7]

MORE **VULNERABLE**

Cybersecurity has often been underfunded, leaving healthcare organizations more vulnerable to attack.[8]

CHALLENGE

- Most hospital IT teams **don't have the staff or budget** for around-the-clock cyber monitoring.
- Attacks often happen at night or on weekends, when internal teams may not be watching. Without constant visibility, **threats can escalate before anyone notices**.

SOLUTION

CloudWave combines SentinelOne's autonomous detection and response with a healthcare-focused SOC to deliver 24x7 expert coverage. Our analysts **monitor, investigate, and remediate threats** on behalf of hospital teams, acting as an extension of internal staff.

SentinelOne

MANAGED EDR: BUILDING A STRONGER CYBER DEFENSE FOR HEALTHCARE

CloudWave's Managed EDR service was built specifically for the realities of healthcare. It combines continuous endpoint monitoring, AI-driven detection, and rapid response capabilities to stop threats before they disrupt operations.

CloudWave helps hospitals stay ahead of attackers, meet compliance requirements, and safeguard the integrity of patient care.

LEARN MORE →

LEARN MORE AT

GoCloudWave.com | in

CloudWave

SOURCES

1. IBM, When ransomware kills: Attacks on healthcare facilities
2. Microsoft, U.S. Healthcare at risk: Strengthening resiliency against ransomware attacks
3. The HIPAA Journal, 63% of Known Exploited Vulnerabilities Can be Found in Hospital Networks
4. Department of Health and Human Services, Hospital Cyber Resiliency Initiative Landscape Analysis Landscape Analysis
5. HIMSS, 2023 HIMSS Healthcare Cybersecurity Survey
6. HIPAA Journal, Healthcare Compliance Teams Stretched Thin Due to Complex Regulations and New Risks
7. Microsoft, U.S. Healthcare at risk: Strengthening resiliency against ransomware attacks
8. Microsoft, U.S. Healthcare at risk: Strengthening resiliency against ransomware attacks