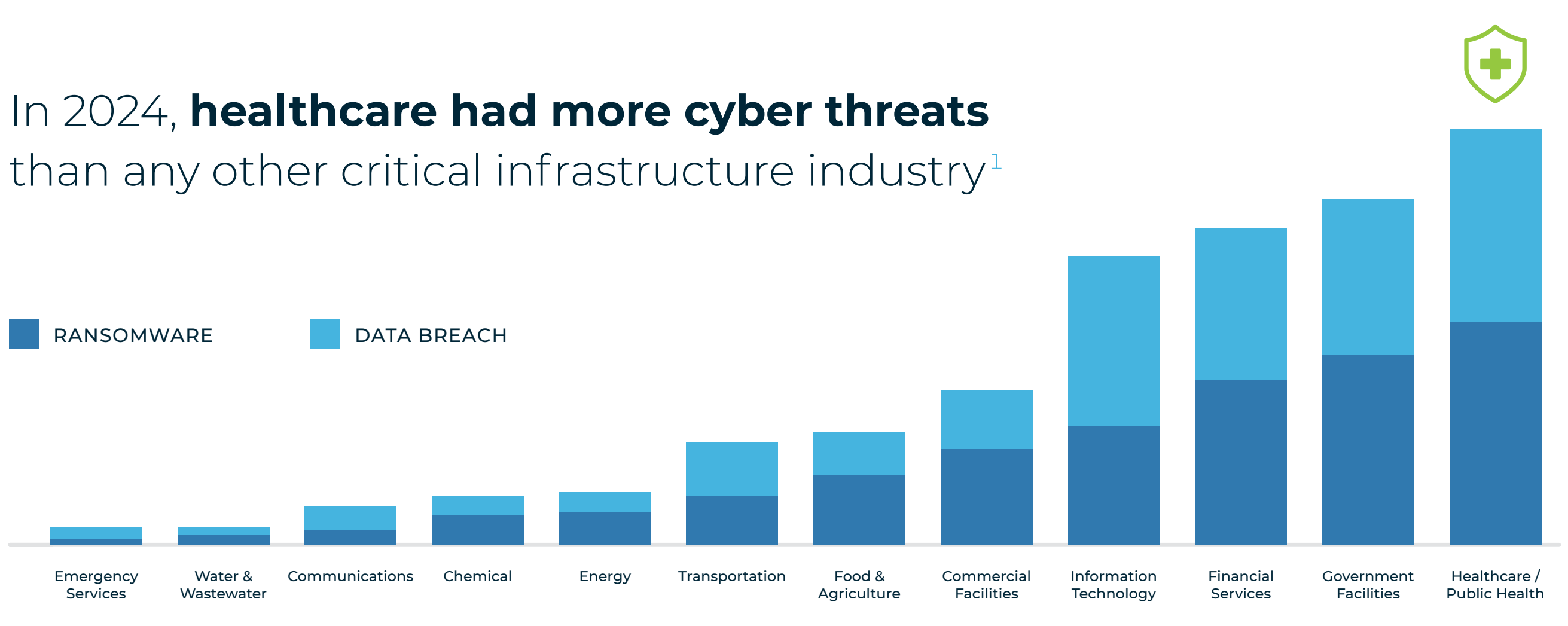
CloudWave

Cutting Through the Noise

How Healthcare Managed Detection and Response (MDR) Protects What Matters

Healthcare Continues to Face Relentless Cyber Threats

In 2024, **healthcare had more cyber threats** than any other critical infrastructure industry[1]



444
REPORTED INCIDENTS

238 RANSOMWARE — **206** DATA BREACH

A total of 444 reported incidents impacted healthcare, comprising 238 ransomware threats and 206 data breach incidents[2]

25.6M
HEALTHCARE RECORDS COMPROMISED

Confirmed incidents affecting healthcare providers compromised 25.6 million healthcare records[3]

$5.7M AVERAGE RANSOM DEMAND

$900K AVERAGE RANSOM PAID

The average ransom demand in these cases was $5.7 million, while the average ransom paid amounted to $900,000[4]

$9.77M
AVERAGE DATA BREACH COST

Average cost of a healthcare data breach was $9.77 million in 2024[5]

Alert Overload!

Healthcare organizations have invested in a range of cybersecurity tools designed to detect threats early—but these solutions often create an unintended consequence: **alert fatigue**.

Thousands of cybersecurity alerts/week

The average hospital faces thousands of cybersecurity alerts per week[6], ranging from **phishing** attempts to **anomalous logins** and **malware detections**

5,000+ security alerts each day

Some organizations even receive as many as 5,000+ security alerts **each day**[7]

74% threats ignored

A study by the Ponemon Institute found that security teams **ignore or do not have time to respond** to 74% of security alerts[8]

Tune them out

When professionals, such as cybersecurity practitioners or clinicians, are **exposed to repetitive, non-urgent signals**, they begin to tune them out[9]

"Alert storming"

Malicious actors have learned to weaponize alert fatigue, launching **high volumes of low-priority events to distract analysts** and hide malicious activity in plain sight—referred to as "alert storming"[10]

Alert fatigue is a serious and silent threat to hospital cybersecurity. Most healthcare IT teams are overwhelmed by noise — and **the real risks are getting overlooked**.

The Problem: Volume Without Context

High alert volumes don't just bury teams in noise—they also obscure what truly matters. Without context, it's nearly impossible to distinguish real threats from false positives.

False Positives + Noise = Slower response and missed threats

Many healthcare organizations rely on outdated threat detection systems that cannot contextualize alerts. This makes prioritization difficult and increases the risk of dismissing critical incidents. An alert marked "low-priority" may actually be the first sign of a serious breach—but without real-time threat intelligence and contextual analysis, that signal is easy to miss until it's too late.

THE RESULT?

- **Costly Oversights**
- **Delayed Containment**
- **Greater Exposure to Risk**

Why Traditional Detection Fails in Hospitals

It doesn't distinguish a radiology workstation from a receptionist's PC

Flags normal ICU logins as anomalies

Misses the clinical importance of the asset at risk

Everything looks urgent — nothing gets resolved fast enough.

Managed Detection and Response (MDR), Built for Healthcare

Managed Detection and Response (MDR) is purpose-built to address these gaps. Unlike cybersecurity solutions that focus solely on prevention, **MDR delivers 24/7 threat monitoring, rapid detection, and real-time response** to active threats—before they can cause harm.

For healthcare organizations, MDR doesn't just reduce alert fatigue—it helps cybersecurity teams focus on what matters most. By filtering out noise and surfacing high-priority threats with context, MDR improves incident response, strengthens compliance, and supports patient safety—**all without overburdening existing healthcare IT staff**.

What Makes CloudWave MDR Different

It's tuned for care, not just code

CARE — Google SecOps — CODE

- **Context-Aware Prioritization**
  Knows which systems matter to care delivery
- **Noise Suppression**
  Reduces false positives by up to 90%
- **Healthcare-Tuned SOC**
  Analysts trained in hospital workflows
- **Google SecOps for Speed & Scale**
  Automated playbooks, forensic visibility, fast containment
- **Real-Time Protection**
  MDR that *responds*, not just alerts

A Day in the Life with CloudWave MDR

CLOUDWAVE MDR

1,200 Alerts → **2 Alerts** → **Contained within minutes**

A lateral movement attempt is buried in 1,200 alerts

CloudWave's MDR platform **flags just two**

Within minutes, the device is contained, credential reuse is blocked, and the customer receives a full forensic report — **without alert fatigue**

In healthcare, every second counts.
You don't need more alerts. You need an MDR that understands your environment — and knows what not to alert on.

CloudWave MDR: Built for Hospitals. Tuned for Patient Safety

24x7 SOC

HEALTHCARE-TRAINED ANALYSTS

RISK-DRIVEN ALERT TRIAGE

SMART RESPONSE AUTOMATION

Let's Cut Through the Noise: Request a Demo or Risk Assessment

CONTACT US →

READ OUR BLOG

Cutting Through the Noise: How Healthcare MDR Prioritizes What Matters, to learn more.

READ OUR BLOG →

LEARN MORE AT

GoCloudWave.com | in

CloudWave

SOURCES

1. American Hospital Association, Federal Bureau of Investigation Internet Crime Report 2024
2. American Hospital Association, Federal Bureau of Investigation Internet Crime Report 2024
3. The HIPAA Journal, 2024 Was Another Bad Year for Healthcare Ransomware Attacks
4. The HIPAA Journal, 2024 Was Another Bad Year for Healthcare Ransomware Attacks
5. IBM, Cost of a Data Breach (2018-2024)
6. IBM, What is Alert Fatigue?
7. CIO, 7 key findings from Cisco's CISO benchmark study
8. Ponemon Institute
9. American Journal of Nursing, Original Research: Alarm Fatigue: Exploring the Adaptive and Maladaptive Coping Strategies of Nurses
10. IBM, What is Alert Fatigue?