Four Reasons Healthcare Attracts Cybercriminals

And What You Can Do

Healthcare organizations are some of the most targeted entities in the world when it comes to cybercrime. With an expanding digital footprint, critical systems that can't tolerate downtime, and highly valuable personal health data, the healthcare sector presents unique opportunities for threat actors and unique challenges for defenders.

From large provider networks to small hospitals, many struggle with outdated technology, limited staff, and insufficient visibility. Meanwhile, ransomware, insider threats, and device-level exploits continue to rise. Below are four structural issues that contribute to healthcare's persistent vulnerability, along with practical steps your organization can take to better defend itself.

1. Understaffed and Underfunded Security Programs

Healthcare security teams are expected to manage an increasingly complex environment, often with limited resources. Historically, the sector allocated just 4–7% of IT budgets to cybersecurity.[1] That number is increasing; recent data shows the average now hovers around 7%, with many health systems budgeting 7–10% or more, depending on size, digital maturity, and regulatory exposure.[2,3,4]

Still, the resource gap remains. Small security teams must manage legacy infrastructure, navigate regulatory audits, and investigate threats across sprawling networks and medical device ecosystems. Many rely on security information and event management (SIEM) deployments that are slow, siloed, and labor intensive, slowing detection and increasing risk.

Low staffing levels and alert fatigue are a dangerous combination. In many hospitals, a single security incident can take days to fully investigate due to manual triage and fragmented log data. That delay gives attackers time to escalate privileges, deploy ransomware, or exfiltrate patient data undetected.

What You Can Do

- Automate detection and triage workflows to reduce analyst burden.
- Prioritize detection aligned to MITRE ATT&CK® to ensure relevant threat coverage.
- Deploy security controls that work across hybrid environments to close gaps in visibility.
- Leverage prebuilt content for compliance and risk reporting to reduce audit prep time.

[1] USA Department of Health and Human Services, Healthcare & Public Health Sector Coordinating Councils. (2018, December 27). *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients.* https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf
[2] McKinsey & Company. *Cybersecurity in healthcare: The coming transformation.* 2023.
[3] Becker's Health IT and CIO Report. *How much are hospitals budgeting for cybersecurity in 2024?* April 2024.
[4] HIMSS. *2025 HIMSS Healthcare Cybersecurity Survey*.

2. Rapid Growth in Telehealth and Distributed Care

Telehealth adoption exploded during the pandemic and continues to expand. Virtual care models, remote diagnostics, and patient monitoring solutions have introduced new data flows, platforms, and APIs into already complex environments. While these tools improve access and efficiency, they often come with inconsistent security monitoring and fragmented integration with the security operations center (SOC).

In a typical telehealth deployment, traffic and user flow across cloud providers, mobile apps, third-party platforms, and internal systems, many of which lack centralized logging or identity federation. In this environment, an attacker can exploit misconfigured permissions, intercept data in transit, or use a compromised account to move laterally

Healthcare organizations also face pressure to deliver care faster and manage more patients per day. This can lead to shortcuts in access controls, unmonitored privileged accounts, or overlooked endpoint exposures, especially in mixed-use environments shared between clinical and administrative users.

What You Can Do

- Establish centralized log ingestion from telehealth platforms, cloud environments, and EHR systems.
- Correlate events across disparate data sources to build a unified picture of user activity.
- Automate anomaly detection to identify lateral movement or abuse of telehealth services.
- Maintain visibility into identity, role, and context for all users and devices interacting with patient data.

3. An Expanding Attack Surface of Connected Medical Devices

Modern hospitals depend on an ever-growing number of connected medical devices, from infusion pumps and ventilators to imaging equipment and telemetry systems. These devices enhance clinical efficiency but also expand the attack surface.

According to a 2023 report, over 50% of connected medical devices contain known critical vulnerabilities and most are difficult or impossible to patch.[5] Many operate on outdated firmware, use insecure protocols, or lack native logging entirely. Attackers increasingly exploit these visibility gaps to establish footholds inside hospital networks.

A successful exploit on a vulnerable device can lead to privilege escalation, lateral movement, or data theft. Worse, it can interrupt patient care if clinical systems are disrupted. As attacks grow more sophisticated, simply segmenting medical devices on a separate VLAN is no longer enough.

What You Can Do

- Perform a complete inventory of all connected devices, including model, firmware, and network behavior.
- Use passive traffic analysis to detect abnormal activity without installing agents.
- Apply behavior-based detection to identify deviations from known-good communication patterns.
- Enrich device data with user and asset context to improve investigation accuracy.

4. Medjacking: A Persistent and Underreported Threat

Medjacking—short for medical device hijacking—is the exploitation of vulnerable or improperly secured medical equipment to gain access, disrupt operations, or exfiltrate data. These attacks may begin with compromised IoT devices, third-party monitoring tools, or even physical access in a clinical setting.

In one common scenario, an attacker compromises a device with weak authentication, then uses it to pivot to critical systems like EHR databases or imaging archives. In more advanced cases, malicious actors manipulate device configurations to disrupt care or conceal data exfiltration activities.

The challenge is that many of these devices lack audit logs or endpoint protection. Security teams often don't know a device is compromised until operational anomalies or patient safety issues arise.

What You Can Do

- Establish real-time telemetry monitoring for devices and endpoints that cannot support traditional agents.
- Use dynamic watchlists to track high-risk users, assets, and zones based on evolving threat context.
- Implement continuous validation of logging pipelines to detect silent failures in data collection.
- Cross-reference device behavior with user activity to identify insider threats and credential misuse.

[5] *InformationWeek* (Nov 2023)

The Path Forward: Better Visibility, Faster Action, Stronger Outcomes

Healthcare organizations face a perfect storm of risk factors: constrained resources, fragmented visibility, and a growing reliance on connected systems. At the same time, attackers are getting faster and the consequences of a breach are more severe.

The solution isn't just spending more. It's spending smarter:

- Invest in automation and machine learning to reduce reliance on manual processes.
- Focus on outcome-based use cases that align with real-world threats.
- Enable faster investigations by consolidating context and eliminating silos.
- Close detection gaps using benchmarks like the ATT&CK framework.

How Exabeam Helps

Exabeam supports healthcare organizations looking to modernize security operations without increasing analyst workload or overhauling your security stack.

The New-Scale Security Operations Platform (sold as Exabeam Fusion) provides:

- Machine-learned threat detection that surfaces anomalies across users, assets, and devices
- Dynamic risk scoring that prioritizes threats based on behavior, context, and business impact
- Automatically generated timelines and case summaries to accelerate investigations
- Prebuilt compliance content for HIPAA, NIST, ISO, and more
- Silent log source monitoring to ensure uninterrupted visibility
- Flexible deployment options starting at 25GB/day, designed for health systems of all sizes

Want to Dive Deeper?

Download the guide, Four Emerging Phishing Techniques and How to Detect Them, to learn more about the latest phishing techniques and how to protect your organization from these threats.

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam

Learn more at www.exabeam.com →