Presented by

Trellix ADVANCED RESEARCH CENTER

TRELLIX HEALTHCARE CYBERSECURITY THREAT INTELLIGENCE REPORT

Analysis Period: January 1 - December 31, 2025
Sector Focus: Global Healthcare
Classification: TLP: White

TABLE OF CONTENTS

EXECUTIVE SUMMARY

For decades, hospitals and healthcare providers relied on largely isolated clinical systems designed first and foremost for patient safety, not cybersecurity. Many medical devices operated in closed environments, with limited connectivity and minimal exposure to external threats, a reality reflected in early research, including Trellix investigations into network-exposed patient monitoring systems.

Today, that model has undergone a fundamental change. Healthcare is rapidly embracing cloud platforms, remote access, and internet-connected medical devices to drive efficiency, interoperability, and quality of care. This innovation is inherently positive, but it also expands the attack surface, exposing clinical technology to threats it was never engineered to withstand. As artificial intelligence accelerates digital transformation across the sector, the pace of connectivity and with it the risk to patient safety will only continue to grow.

Trellix maintains a large customer base of healthcare organizations, providing a unique vantage point into the current threat landscape. In 2025, our telemetry recorded 54.7 million detections across the multiple Trellix security products installed by our healthcare industry customers. While these detections represent potential security events flagged by our telemetry rather than confirmed successful attacks, they underscore the sheer volume of noise and potential risk filtering through healthcare networks. Notably, of all these global detections, 75% originated from our U.S.-based customers, highlighting the disproportionate targeting of the American healthcare infrastructure.

This year, the industry maintained its position as the most expensive sector for data breaches for the 15th consecutive year. While global breach costs moderated, the United States set a record high of $10.22 million per incident.

The defining trend of 2025 was the "Cascading Effect." A shift where breaches in administrative networks or non-clinical Operational Technology (OT) systems, such as a building’s HVAC, could paralyze an entire health system’s clinical workflow. These disruptions were not merely financial; they were lethal. Research confirmed that hospitals affected by cyberattacks, including cloud/account compromises, supply chain attacks, ransomware attacks, and business email compromise (BEC) incidents, saw a 29% increase in mortality rates for inpatients, and neighboring hospitals experienced an 81% surge in cardiac arrest cases due to emergency diversions.

THE FINANCIAL REALITY OF CARE DISRUPTION

The financial toll of 2025 was not merely the result of record-breaking ransoms but the massive, unpredictable cost of systemic operational failure.

According to the IBM 2025 Report, average healthcare breach costs fell to $7.42 million from $9.77 million in 2024. Despite this drop, healthcare remains the costliest sector for the 14th consecutive year, largely due to rigid regulatory requirements like HIPAA and a 279-day detection and containment cycle—the longest of any industry studied by IBM.

- The Black Market Premium: A single electronic health record (EHR) now sells for approximately $60 on the dark web—nearly 20 times the value of a stolen credit card. This high valuation drives the volume of "quiet" exfiltration attacks. Further highlighting this premium, Trellix observed a threat actor offering medical records for a US healthcare provider for $250 per compromised account in late 2023, demonstrating that specialized or high-integrity clinical datasets can command prices far exceeding general black-market averages.
- Cost Breakdown (Average Per Breach):
    - Detection and Escalation: $1.47 million.
    - Lost Business (Downtime/Reputation): $1.38 million.
    - Post-Breach Response (Legal/Notifications): $1.2 million.

For healthcare systems, "time is money" takes on a literal and devastating meaning. Industry benchmarks from Comparitech and Censinet indicate:

- Per Minute Cost: Between $7,500 and $9,000.
- Per Day Cost: An average of $1.9 million in lost revenue and recovery expenses.
- The Duration Crisis: The average healthcare organization faced 17+ days of downtime per attack in 2025, with some major systems experiencing partial outages for months. 76% of organizations reported that full recovery from a major attack took longer than 100 days.

The financial ripples of a major third-party clearinghouse breach (carrying over into early 2025 reports) provided a blueprint for total industry disruption. A parent company reported that total costs for that single incident would likely exceed $2.9 billion.

The AMA's 2025 analysis found that 80% of physician practices lost revenue from unpaid claims, and 55% had to use personal funds to cover practice expenses. For smaller facilities, a $200,000 loss—which quadrupled in frequency in 2025—is often the difference between survival and closure.

Regulatory and Long-term Financial Impact

- The Price Hike Effect: To absorb these staggering costs, nearly half of breached healthcare organizations (48%) reported they would be raising the prices of their medical services, with some increases reaching 15% or more.
- HHS-OCR Penalties: Enforcement shifted aggressively in 2025. Federal civil penalties for HIPAA violations now frequently hit the maximum tier for "uncorrected" neglect, with such ongoing violations costing up to $1.5 million.

Key Financial Metrics

- Average Cost of US Breach: $10.22 Million (up 9.2% from 2024).
- Downtime Cost: Modern hospital operations lose approximately $9,000 per minute during a total system outage.
- Detection & Escalation: These costs averaged $1.47 million per incident, reflecting the difficulty of finding "quiet" actors in complex clinical networks.

THE 2025 ADVERSARY PROFILE: FROM RANSOMWARE TO PATIENT EXTORTION

Adversaries in 2025 moved beyond simple encryption to "triple extortion" data theft, service disruption, and individual patient harassment. The Ransomware-as-a-Service (RaaS) ecosystem underwent a violent reorganization following the high-profile fallout of the Change Healthcare breach, leading to more aggressive, affiliate-centric models.

The scale of adversarial activity in 2025 remained high, as evidenced by Trellix telemetry and targeted campaign tracking. This data reveals a persistent, high-volume threat environment specifically tuned to the healthcare sector's unique vulnerabilities.

Trellix Telemetry and Intelligence

- Total Detections: Trellix recorded 54.7M total detections across its healthcare related customer organizations globally throughout 2025.
- Trellix Email Security accounted for 85% of the total amount of detections.
- Geographic Concentration: The United States remained the primary epicenter of this activity, accounting for 75.14% of all healthcare detections.

Active Threat Operations (Campaign Tracking)

- Targeted Campaigns: Our Advanced Research Center has identified 109 unique campaigns specifically engineered to compromise healthcare infrastructure in 2025.
- Activity Peaks: Trellix telemetry observed the most activity in the first half of 2025, with some isolated spikes on email detections in January and March.

Threat Actor Deep-Dive

Qilin: Qilin matured into a high-tempo operation in 2025, focusing on double-digit monthly victim postings. They are known for their sophisticated Linux and ESXi-capable payloads, which target the back-end servers housing critical EHR databases.

- Incident Highlight: In May 2025, a large U.S. hospital system suffered a massive Qilin attack impacting 478,188 patient records. The group exfiltrated 852 GB of data (1.35 million files). Qilin is infamous for its "patient extortion" tactic, where they bypass the provider and text patients directly with their diagnostic results, demanding a "privacy fee" to prevent public disclosure.

INC Ransom: Emerging as one of the most prolific healthcare-targeting operations in 2024-2025, INC Ransom demonstrated remarkable consistency with 34 observed attacks, accounting for 7.9% of all healthcare attacks. Their healthcare targeting peaked in 2025, representing a significant portion of their total operations.

- Incident Highlight: Based on ransomware victim posts tracked by Trellix's Enriched Ransomlook dataset, in 2025, INC Ransom executed healthcare campaigns. These included high-profile targets such as a regional hospital in North America, a national public health system, and a major hospital in the Southern Hemisphere.

Devman2: Operating with devastating efficiency since late 2024, Devman2 has established itself as a major threat to international healthcare infrastructure with 26 observed attacks, representing 6.1% of all healthcare attacks. The group is notorious for massive data exfiltration, with individual healthcare breaches consistently ranging from 200GB to 300GB of stolen patient data per incident.

- Incident Highlight: Based on ransomware victim posts tracked by Trellix's Enriched Ransomlook dataset, December 2025 marked Devman2's most aggressive healthcare campaign, claiming 23 healthcare victims in a single month. Their attack on a major Chilean private healthcare network resulted in the theft of 250GB of data. Simultaneously, they breached a hospital in France (221GB) and a U.S. provider (300GB, including QuickBooks financial dumps).

Sinobi: Despite emerging as recently as July 2025, Sinobi rapidly established itself as a significant threat with 21 observed attacks, representing 4.9% of all healthcare attacks. Their rapid emergence and immediate focus on specialized firms like biotech suggest either experienced operators launching a new brand or sophisticated initial access capabilities.

- Incident Highlight: Based on ransomware victim posts tracked by Trellix's Enriched Ransomlook dataset, Sinobi's October 2025 "blitz" resulted in 13 healthcare victims in a single month, ranging from pharmaceutical manufacturers to individual dental practices. And already in January 2026, they have begun operations with the targeting of a specialized life science firm and an aging services division, showing an evolution toward high-value healthcare technology and specialized care providers.

Medusa: Maintaining steady healthcare operations throughout 2024-2025, Medusa claimed 18 observed attacks, accounting for 4.2% of all healthcare attacks. The group is distinguished by their detailed data quantification and systematic targeting of major pharmaceutical corporations and mental health providers.

- Incident Highlight: Based on ransomware victim posts tracked by Trellix's Enriched Ransomlook dataset, Medusa's September 2025 breach of a major pharmaceutical company resulted in the exfiltration of 478.2GB of data—one of the largest pharmaceutical breaches of the year. Their targeting of organizations handling the most protected health information under HIPAA was highlighted by attacks on a regional mental health authority and a specialized HIV/AIDS care provider.

Interlock: Emerging in late 2024, Interlock has quickly established itself as a sophisticated threat to critical infrastructure, with a distinct focus on the North American healthcare sector. The group is notable for its "uncommon" initial access tactics, frequently using drive-by downloads on compromised legitimate websites that push fake browser updates (e.g., Chrome or Edge) or security software patches to deploy their proprietary Interlock RAT. They operate a double-extortion model, often specifically targeting virtual machine (VM) environments and leveraging legitimate tools like AzCopy to exfiltrate massive datasets to cloud storage before triggering encryption.

- Incident Highlight: In early 2025, Interlock targeted a kidney dialysis giant, exfiltrating approximately 1.5 terabytes of data from its laboratory databases. This breach ultimately impacted 2.7 million individuals, exposing names, social security numbers, and clinical treatment records. Interlock has been directly implicated in high-impact disruptions at regional health systems, where the resulting system downtime forced the cancellation of elective procedures and created significant risks to patient safety.

RansomHub: In early 2025, RansomHub was one of the most impactful groups targeting the healthcare sector. Their success was driven by a revolutionary affiliate model: offering a 90% commission and allowing affiliates to handle ransom transactions directly. This attracted elite talent from defunct groups like ALPHV/BlackCat.

- Incident Highlight: RansomHub claimed responsibility for several high-capacity breaches, including the Latin American division of a major insurance company and a large business associate, resulting in the potential exposure of millions of records. Their tactics favor exfiltration-only attacks, which tripled in frequency in 2025 as groups realized that threatening to leak medical data is more effective than the technical hurdle of encryption.

Cl0p: In late 2025, the Cl0p ransomware gang executed a massive campaign targeting on-premises Oracle E-Business Suite (EBS) systems. By exploiting CVE-2025-61882 and CVE-2025-61884 as zero-days for months before patches were released, they compromised nearly 30 major organizations, including those in the healthcare supply chain. Their strategy focuses on "mass victimization" via widely used enterprise software rather than individual hospital targets.

Rhysida: Rhysida remained a significant threat, maintaining a strong healthcare focus throughout the year. They are known for a "double-jeopardy" approach, often using a tight 7-day payment window before publishing data.

- Incident Highlight: In mid-2025, Rhysida added a specialized surgical center and a regional medical group to its leak site, claiming the theft of SQL databases and insurance cards. CISA updated its #StopRansomware advisory on Rhysida in April 2025 to account for their new "CleanUpLoader" and "OysterLoader" initial access tools.

Strategic Trend: The "Patient Extortion" Game

According to the Health-ISAC 2025 Threat Landscape Report, patient extortion has continued to be a mainstream revenue stream for cybercriminals.

- Economics of Small-Batch Extortion: By demanding just $50 to $500 per patient, actors bypass corporate insurance and legal teams. In 2025, extortion-only attacks to healthcare providers was observed in 12% of all healthcare attacks, representing a 300% increase since 2023.

The RaaS Economic Shift

A surprising trend in 2025 was the drop in average ransom payments. While volume remained high, the average ransom payment in healthcare plummeted from $1.47 million to $150,000. This reflects a shift toward mid-range demands ($1M - $5M) being negotiated down significantly, as only 36% of providers chose to pay in 2025—a record low.

LANDMARK HEALTHCARE CYBERSECURITY INCIDENTS IN 2025

In 2025, the U.S. Department of Health and Human Services (HHS) disclosed about 516 breaches, impacting more than 35.5 million individuals. Each breach represents more than just data on a spreadsheet; it means patients facing uncertainty about their privacy and organizations scrambling to restore trust.

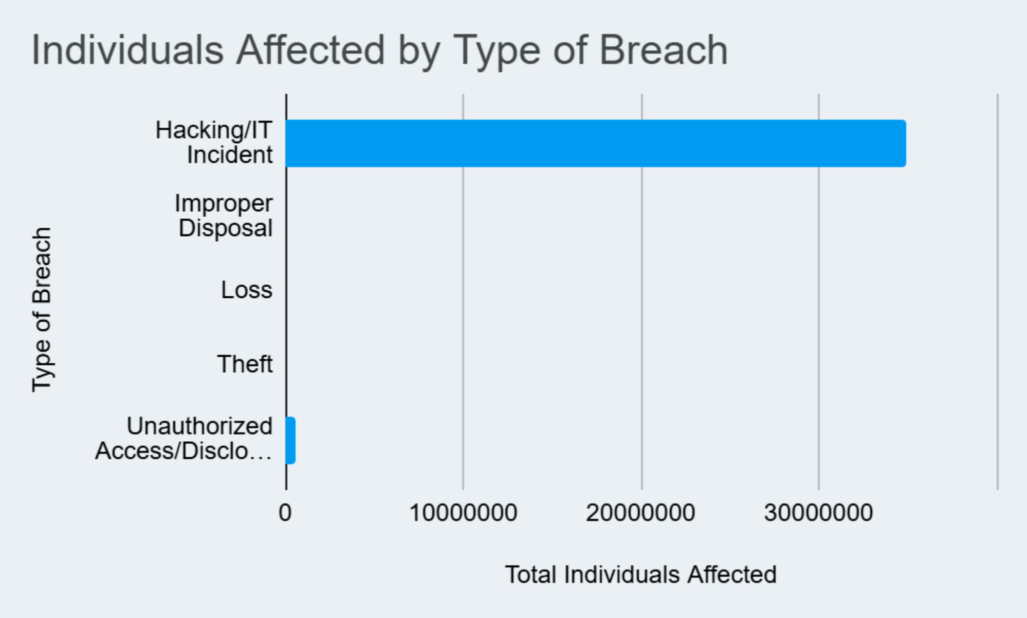
Key Takeaways from the Breach Report Data

Hacking/IT Incidents are the Dominant Threat and Primary Driver of Impact

Hacking/IT Incidents are overwhelmingly the most frequent and impactful type of breach in the dataset, both in terms of sheer number of events and the number of individuals affected.

- High Frequency: 410 out of the 516 total breaches (79%) were classified as Hacking/IT Incidents.
- Massive Scale of Impact: This breach type accounted for 34.9 million of the 35.5 million total individuals affected (over 98% of the total impact).
- Location: The primary location for the breach was the Network Server (306 incidents), followed by Email (120 incidents), aligning with the nature of Hacking/IT Incidents.

The chart below illustrates how much larger the impact of Hacking/IT Incidents is compared to all other types of breaches.



Source: (U.S. Department of Health and Human Services Office for Civil Rights Breach Portal)

Healthcare Providers Face More Frequent Breaches, but Business Associates' Breaches Affect More People on Average

While Healthcare Providers have the highest frequency of breaches, breaches involving Business Associates tend to be larger in scale, affecting a significant portion of the total individuals compromised.

- Frequency: Healthcare Providers reported 360 breaches, significantly more than the 101 reported by Business Associates.
- Impact Distribution: Breaches involving Healthcare Providers affected about 19.1 million individuals, while those involving Business Associates affected a nearly comparable 15.4 million individuals.
- Implied Average Size: This difference in frequency versus total impact suggests that an average breach involving a Business Associate affects a larger number of individuals than an average breach involving a Healthcare Provider.

Unauthorized Access/Disclosure is the Second Most Common Issue, but with Much Lower Individual Impact

While Hacking/IT Incidents dominate, the next most common issue is a clear operational or process-related problem: Unauthorized Access/Disclosure.

- Second Most Frequent: Unauthorized Access/Disclosure accounted for 85 incidents, making it the second most frequent type of breach.
- Limited Individual Impact: Despite its frequency, this breach type affected only 580,976 individuals, a tiny fraction of the individuals affected by Hacking/IT Incidents.

Notable Incidents

Major Academic Health System Compromise: 5.5 Million Patients Exposed

In March 2025, a major academic health system discovered unusual activity on its IT network. This quickly escalated into the largest healthcare breach of 2025, affecting 5.5 million people.

- Details: Attackers exfiltrated sensitive demographic details and Social Security numbers. While clinical systems remained intact, the sheer scale led to an $18 million settlement later in the year to cover litigation and administrative costs.

Supply Chain Disruption via Business Associate: 5.4 Million Records

Between late January and early February 2025, a large business associate suffered a ransomware-driven intrusion. As a key partner for giants in the sector, the breach compromised data from 5.4 million individuals.

- Supply Chain Impact: The ripple effect was massive; multiple partners had to report separate incidents.

Major Dialysis Provider Impacted by Ransomware : 1 Million Impacted

A kidney dialysis giant fell victim to the Interlock Ransomware group between March and April 2025.

- Impact: The group exfiltrated 1.5 terabytes of data, including medical records and tax IDs.
- Cost: The provider disclosed $13.5 million in direct costs in SEC filings, primarily for remediation and system restoration.

Large Health Plan Misconfiguration: 4.7 Million Member Misconfiguration

In April 2025, a major U.S. health plan provider disclosed a significant privacy incident affecting 4.7 million members. This was not a hack, but a misconfiguration of an advertising service.

- Details: For nearly three years, sensitive member data (including "Find a Doctor" searches) was shared with the advertising service, potentially allowing for targeted advertising based on protected health information.

Identity Attack on a Major Brokerage Firm: 1.1 Million Records

This incident, disclosed in early 2025, involved a targeted identity attack against a large insurance brokerage. Adversaries gained access to a single employee's computer for just a few hours. In that window, they exfiltrated the data of 1.12 million individuals.

- Details: A prime example of why Identity Threat Detection and Response (ITDR) and session-token protection are critical components of a modern healthcare security stack.

TACTICS, TECHNIQUES, & PROCEDURES (TTPS)

While the sabotage of external lifeline sectors creates a profound "trickle-down" effect on hospital availability, threat actors are simultaneously perfecting the "Clinical Pivot"—a method of moving from internal administrative networks directly into the clinical environment. This convergence represents a fundamental shift where cybersecurity in healthcare is no longer just a technology problem, but a patient safety imperative. The following section details the specific Tactics, Techniques, and Procedures (TTPs) used to exploit the IT-to-clinical boundary, mirroring the infrastructure disruption strategies observed in broader critical infrastructure campaigns.

Initial Access

Phishing (T1566.001): Still the primary vector (89%), but evolving. Actors are now using "AI Transformation" and "Regulatory Compliance" themes to trick administrative staff.

VPN Exploitation (T1133): The exploitation of SonicWall (CVE-2024-40766) and Fortinet devices became a standard entry point for Akira.

Credential Access

Credential Dumping (T1003.001): Mimikatz and LaZagne are used to dump LSASS memory from nurse workstations to steal domain credentials.

Discovery & Lateral Movement

Living-off-the-Land (LotL): Attackers abuse native tools to map the clinical network.

- WMI Queries: Get-WMIObject -Class Win32_NetworkAdapter is used to identify medical devices based on MAC address vendors (e.g., GE, Siemens).
- PowerShell: Used to execute remote commands on PACS (Imaging) Servers, which often sit at the intersection of IT and Clinical networks.

Impact (Data Destruction)

ESXi Encryption (T1486): By targeting the hypervisor, actors can encrypt hundreds of virtual machines simultaneously. This is particularly devastating in healthcare, where EHRs, PACS, and Lab Systems are often virtualized on the same cluster.

Technical Indicators and TTPs

Command and Control Infrastructure (Source: Campaigns + Detections)

Domain Patterns:

- Healthcare-themed domains: medical-update[.]com, hipaa-compliance[.]org
- Typosquatting: microsft-teams[.]net, zoom-healthcare[.]com
- Subdomain abuse: Legitimate healthcare domains with malicious subdomains.

Network Indicators:

- Beaconing Patterns: 60-second intervals to mimic legitimate medical device communications.
- Data Exfiltration: HTTPS tunneling disguised as software updates.
- Persistence Mechanisms: WMI event subscriptions, scheduled tasks named after medical processes.

File-based Indicators:

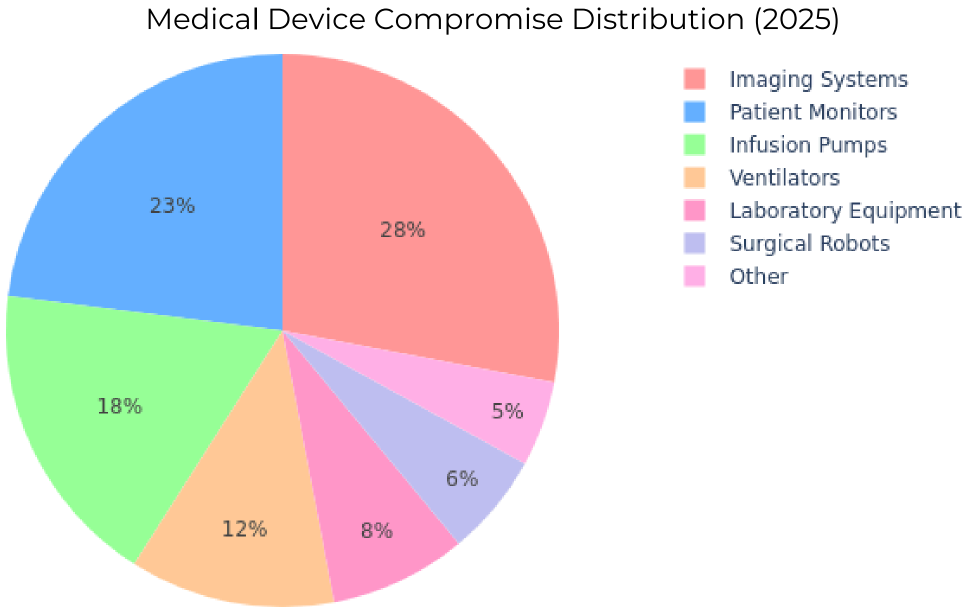
- Malware Families: Cobalt Strike beacon, Metasploit payloads, custom PowerShell frameworks.
- Naming Conventions: Files disguised as medical software: MedicalDeviceUpdate.exe, HIPAACompliance.pdf.exe.
- Persistence Locations: %PROGRAMFILES%\Common Files\Medical\, registry keys mimicking medical software.

THE VULNERABILITY MATRIX: IoMT AND OT EXPOSURE

The healthcare attack surface in 2025 is no longer confined to traditional endpoints like laptops and servers. Instead, it is a complex web of Internet of Medical Things (IoMT) and Operational Technology (OT), where 99% of hospitals now manage at least one device with a Known Exploited Vulnerability (KEV).

Medical devices frequently harbor a higher density of security flaws compared to standard enterprise hardware, with 6.2 software bugs per device on average.

- Infusion Pumps: Large-scale analysis of 200,000 infusion pumps in 2025 revealed that 75% possessed one or more known security gaps. Over half were susceptible to critical 2019 CVEs in firmware, and many continue to run legacy firmware with hard-coded or default passwords, making them ideal targets for lateral movement.
- Medical Imaging (DICOM/PACS): Radiology equipment, including CT and MRI scanners, remains a primary target due to its reliance on outdated operating systems. Research shows that 32% of DICOM/PACS workstations had at least one critical unpatched vulnerability, while 20% of imaging systems carried KEVs actively utilized by major ransomware gangs.
- Patient Monitors & Vital Sign Controllers: These devices frequently lack basic security protections and can serve as gateways to broader networks. A notable 2025 disclosure for the Contec Health CMS8000 revealed it transmitted plain-text patient data to a hard-coded public IP address by default, effectively serving as a backdoor for data leakage.



Medical Device Exploitation (Source: Detections + Underground)

2025 Critical Vulnerability & CVE Breakdown

The following vulnerabilities were identified or extensively exploited in the healthcare sector throughout 2025, posing significant risks to clinical operations:

- Contec Health CMS8000 (CVE-2025-0683): This critical vulnerability involves an embedded backdoor within the firmware of patient monitors. In its default configuration, the device transmits plain-text patient data to a hard-coded public IP address, allowing unauthorized remote actors to exfiltrate private health information or take control of the device to perform unintended actions.

- Oracle E-Business Suite (CVE-2025-61882): This multi-stage exploit chain combines authentication bypass and remote code execution to compromise Oracle Concurrent Processing without requiring user credentials. On October 6, 2025, the AHA issued an urgent alert urging immediate action for all hospitals using Oracle EBS. The FBI classified this as a "stop-what-you're-doing and patch immediately" vulnerability, noting its role in large-scale healthcare data theft. High-profile groups like Cl0p ransomware have targeted this flaw to shut down operational back-ends and exfiltrate sensitive employee and financial data from health systems. One of the UK's largest hospital trusts confirmed it was a victim of the Cl0p ransomware gang, which exploited this specific zero-day in August 2025 to steal financial and patient-related invoice data.

- Cisco Secure Email (CVE-2025-20393): This maximum-severity (CVSS 10.0) zero-day vulnerability affects AsyncOS software when the Spam Quarantine feature is enabled. On December 18, 2025, NHS England Digital issued a high-severity alert regarding an ongoing exploitation campaign targeting Cisco Secure Email appliances.

- SonicWall SMA 1000 (CVE-2025-40602): A critical local privilege escalation flaw found in the Appliance Management Console (AMC) due to insufficient authorization checks. Published in December 2025, the NHS England National CSOC assessed future exploitation of this vulnerability as "likely" for healthcare entities. The alert warns that when chained with CVE-2025-23006, this flaw allows for unauthenticated remote code execution (RCE) with root privileges.

The "Legacy Gap": Unsupported Systems in Use

A significant security hole at many hospitals is the reliance on legacy devices that were designed without security in mind.

- End-of-Life (EoL) Dominance: 60% of medical devices in hospitals are end-of-life and lack security patches.
- Unsupported OS: 1 in 5 connected medical devices run on unsupported or end-of-life operating systems.
- Dwell Time: Even when patched, healthcare devices often remain vulnerable for 3.2 years on average.

External Operational Technology (OT) Vulnerabilities and the Hospital Pivot

OT—systems controlling HVAC, elevators, backup power, and pneumatic tubes—provides thousands of entry points for attackers.

- Converged Risk: In 2025, Claroty assessed that 65% of OT systems (BMS, UPS, elevators) have KEVs and are internet-connected.
- The Pivot Path: Adversaries breach unpatched HVAC or electrical controllers to gain a foothold. Once inside, they move laterally to the DICOM imaging networks, effectively paralyzing radiology departments and forcing ambulance diversions. This "OT pivot" bypasses traditional IT security, as these systems rarely host EDR agents.
- USB Threats: OT systems are often "air-gapped," but even if the patching and updating are done via USB, those OT systems may still not be safe. 51% of malware discovered on USB drives in a 2024 study was designed to compromise industrial and operational equipment.

STRATEGIC RECOMMENDATIONS FOR HEALTHCARE SECURITY LEADERS

To counteract the professionalized threat landscape of 2026, healthcare organizations must move from "episodic" security to a unified, risk-based operational strategy.

A cornerstone of this transformation is the development of healthcare-specific threat intelligence capabilities. Leveraging threat intelligence through our Trellix Insights solution and our Trellix Intelligence-as-a-Service (INTaaS) service will allow organizations to move from reactive defense to proactive prediction by identifying threats likely to target their specific environment before an attack occurs. Trellix Insights further enables leadership to prioritize risks based on real-time global sensor data, prescribing actionable remediation steps to optimize the security stance. In addition, the following should be implemented as part of the overall strategy:

- Implement advanced email protection and phishing defense: From our findings, 85% of total detections originating from email telemetry and 89% of initial access were driven by phishing. It is imperative that organizations prioritize layered email controls to disrupt credential theft and malware dropper delivery. Enforce phishing-resistant multi-factor authentication (MFA) for email and remote access, harden mail flow, and use email security to detonate/inspect links and attachments with rapid quarantine and streamlined user-reporting workflows aligned to healthcare lures such as claims, compliance, and AI initiatives.

- Use segmentation and network detection to prevent the “cascading effect” and clinical pivot:

  With 2025 defined by cascading disruptions—where compromise of administrative networks or non-clinical operational technology (OT) (HVAC/building systems/backup power) can paralyze clinical workflows—organizations should implement tiered segmentation across Corporate IT, Clinical IT, Internet of Medical Things (IoMT), and Facilities/OT with default-deny east-west policies. Pair this with network detection and response (NDR) to detect beaconing that mimics device traffic, abnormal DICOM/PACS communications, and HTTPS exfiltration disguised as “updates,” especially for IoMT/OT assets where agents cannot run.

- Strengthen identity governance and session-level monitoring to prevent “quiet” compromise:

  Given the rise of exfiltration-only attacks, patient extortion, and identity-driven incidents, organizations should treat identity as a primary security perimeter. Standardize MFA and least privilege, eliminate shared accounts, implement privileged access management (PAM) and just-in-time (JIT) access for privileged workflows touching electronic health record (EHR) and picture archiving and communication system (PACS) environments, and add identity-focused detections for token/session theft, anomalous admin behavior, and mailbox rule manipulation.

- Deploy endpoint detection and response to stop credential theft and living-off-the-land movement:

  Our report highlighted attackers in 2025 commonly using credential dumping (LSASS) and LotL techniques (PowerShell/WMI) to discover and pivot toward clinical systems. Healthcare organizations should ensure modern endpoint detection and response (EDR) is deployed and actively monitored across corporate endpoints and supported clinical servers/workstations. Prioritize “bridge” assets (PACS/interface engines/jump hosts/virtualization admin endpoints), and operationalize rapid isolation plus credential reset playbooks.

- Prioritize remediation using exploitation likelihood and healthcare-targeted campaigns:

  99% of hospitals are managing at least one device with a Known Exploited Vulnerability (KEV) and high legacy device prevalence. Thus, organizations should run an exploitation-driven vulnerability program. Prioritize KEVs and internet-facing systems (e.g., Oracle EBS, Cisco AsyncOS) and use threat intelligence to translate active campaigns into patch decisions. Where patching is not feasible, apply compensating controls (isolation, virtual patching, credential hardening, protocol-aware monitoring).

- Protect PHI against exfiltration-first operations and patient extortion:

  With adversaries shifting toward triple extortion and patient harassment, and protected health information (PHI) commanding a premium on underground markets, organizations should implement strong data protection and loss prevention controls. Restrict bulk exports and high-risk access paths to PHI repositories, monitor for mass access and unusual application programming interface (API) usage, and apply data loss prevention (DLP) and egress monitoring plus encryption for PHI in transit and at rest—aligned to playbooks designed for exfiltration-only incidents and patient notification scenarios.

- Operationalize SOC-led incident response and resilience to reduce downtime impact:

  With downtime measured in weeks and costs driven by operational disruption, organizations should run a unified detection-to-response workflow that correlates email + EDR + NDR + threat intelligence into predefined playbooks for ransomware, exfiltration-only, and BEC. Validate immutable/offline backups and routine restore testing for EHR/PACS/Lab dependencies, and harden virtualization management to reduce ESXi “blast radius” events capable of disabling hundreds of systems at once.

See more threat reports from

Trellix Advanced Research Center

This document and the information continued herein describes computer security research for educational purposes only and the convenience of Trellix customers. Trellix conducts research in accordance with its Vulnerability Reasonable Disclosure Policy I Trellix. Any attempt to recreate part or all of the activities described is solely at the user's risk, and neither Trellix nor its affiliates will bear any responsibility or liability.

Trellix is a trademark or registered trademark of Musarubra US LLC or its affiliates in the US and other countries. Other names and brands may be claimed as the property of others.