asimily

Connected Device Security and Vulnerability Management for Hospitals

Healthcare delivery organizations (HDOs) continue to be up against a fast-moving landscape trying to keep up with and mitigate cybersecurity threats to medical technology. But even setting aside the immense challenge of safeguarding Internet of Medical Things (IoMT) devices from increasingly sophisticated and frequent attacks, HDOs must also adapt to shifting cyber insurance practices and compliance mandates. All of these challenges are compounded by the budget and staff constraints facing most HDOs. To stay safe, understanding the current state of IoMT security and how to prioritize action is critical.

IoMT devices can prove much more difficult to protect than other IT infrastructures. Patching medical devices in the same way as other hardware is challenging due to regulatory constraints. These devices sometimes run outdated software—which, when paired with the lackluster policy choice by device manufacturers, threatens your security efforts even more.

IoMT device manufacturers have not been held to any external mandates to deliver secure products. As a result, there are more than six vulnerabilities per IoMT device. Proactive manufacturer-led fixes are lacking. More than 40% of IoMT devices at their end-of-life stage had little to no security patches or upgrades. Quite relatedly, HDOs grappling with those countless vulnerabilities—largely in the absence of manufacturer support—were targeted by an average of 43 cyberattacks in 2023, according to a Ponemon Institute study. Almost half of those HDOs suffered a data breach.

HDOs increasingly recognize that limited cybersecurity budgets can't keep up with ever-growing cybersecurity risks. IoMT devices have thousands of vulnerabilities, and HDO cybersecurity teams only have the bandwidth to address a fraction of those risks each month. In response, HDOs are exploring strategies to efficiently reduce risk.

HDOs increasingly recognize that limited cybersecurity budgets can't keep up with ever-growing cybersecurity risks. IoMT devices have thousands of vulnerabilities, and HDO cybersecurity teams only have the bandwidth to address a fraction of those risks each month. In response, HDOs are exploring strategies to efficiently reduce risk.

Top IoMT & IoT Security Challenges

- Growing Attack Surface
- Inaccurate Medical Device & Shadow IoT Inventories
- Legacy Systems & Equipment
- Prioritizing Long Lists of Vulnerabilities
- Underutilized Devices & Equipment
- Staffing Shortages & Skill Gaps

Recent Attacks on Healthcare and the Consequences

Cybercriminals are able to infiltrate hospitals' networks and hold their critical systems hostage for substantial ransoms because of hospital's expanded digital footprint. Ransomware attacks have disrupted emergency services, surgeries, and patient care in hospitals in recent years. Financial fallout from cyberattacks has even forced some hospitals to shut down permanently.

Healthcare companies tend to spend on average 6% of their IT budget on security. This doesn't leave a lot for securing critical systems. When paired with their low tolerance for downtime, healthcare companies and hospitals in particular are very attractive for ransomware groups. In fact, 25% of Americans were impacted by healthcare data breaches in 2023.

Healthcare systems that have started to use more IoT devices, including medicine devices, connected pacemakers, or other Internet of Medical Things (IoMT) devices open themselves up to additional risk. Although the attacks outlined below may not originate with network- accessible and feature-limited devices, the reality is that adding new technology to a healthcare network adds risk.

Healthcare companies will likely continue being attractive targets for threat actors. The personal health information that hospitals and other healthcare organizations store is one of the few pieces of data that can't be changed following a breach. Credit card numbers are only good until financial services firms change them; Social Security numbers cannot be changed and can be readily used for identity theft.

Healthcare organizations would do well to shift some additional spend to cybersecurity, especially in light of the risk of HIPAA fines and a greater focus on data privacy in the year ahead.

A few of the most recent attacks on hospitals

- McLaren Health Care in November 2023 said that a data breach between late July and August affected 2.2 million people. McLaren is a Michigan-based chain of 14 hospitals with revenues of $6.6 billion across the entire system. Through its network, it extends into Indiana as well. The company announced that threat actors had exfiltrated personal data including Social Security numbers, health insurance information, and other personal health data.

- Sutter Health revealed that more than 845,000 customers had their personal data exposed following a breach of its third-party messaging service because of the MOVEit file transfer hack in May. Attackers may have accessed patient's names, birthdates, provider names, health insurance data, treatment cost details, diagnosis, and treatment information but not any financial information or Social Security numbers.

- HCA Healthcare disclosed a data breach in July 2023 that may have affected up to 11 million people in what could be the largest breach of the year. The theft was from external storage used for formatting email messages, according to the company, and didn't include any personal financial or health information. What it did include was patient names, addresses, dates of birth, and information on patient service dates, locations, and the dates for the next appointments.

Unmanaged IoT Devices Leads to Increased Attack Surface and Risk

Shadow IT is one of the most persistent cybersecurity challenges today. Already, researchers estimate that 53% of departments refuse to use IT-approved tools and 80% of workers admit to using SaaS applications at work without getting approval from the IT department.

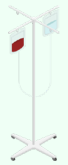
Connected devices often have at least a network interface, like ethernet, Bluetooth, Long-Term Evolution (LTE), Zigbee, Wi-Fi, 5G, or Ultra-Wideband (UWB). Once deployed in a network using these connection methods, IoT systems can be readily discovered and connected to the open internet. This is a major issue because they're not designed to have any setup protocols before connecting to the internet.

Once threat actors gain initial access into a network from a discoverable IoT device, they're able to laterally move deeper into the information architecture to achieve their goals. At the individual device level, IoT equipment is particularly vulnerable to common security pitfalls.

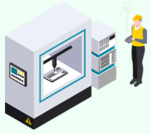
In terms of which categories of connected devices organizations tended to buy, Keyfactor research found that companies tended to deploy the following IoT solutions:

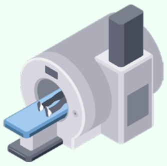
Hybrid work technologies	53%
Security cameras	53%
Real-time monitoring and location tracking	52%
Inventory and asset management	46%
Door locks or physical security	43%
Smart lighting	40%
Space utilization technology/tools	38%
Air quality monitoring	35%

Common Unmanaged IoMT & IoT Devices

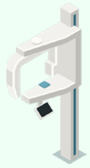

Infusion Pumps

Patient Monitors


Lab Equipment


MRIs

CT Scanners


Xrays

Medical Workstations

Pacemakers

Surgical Robots

Printers & Scanners

Smart TVs

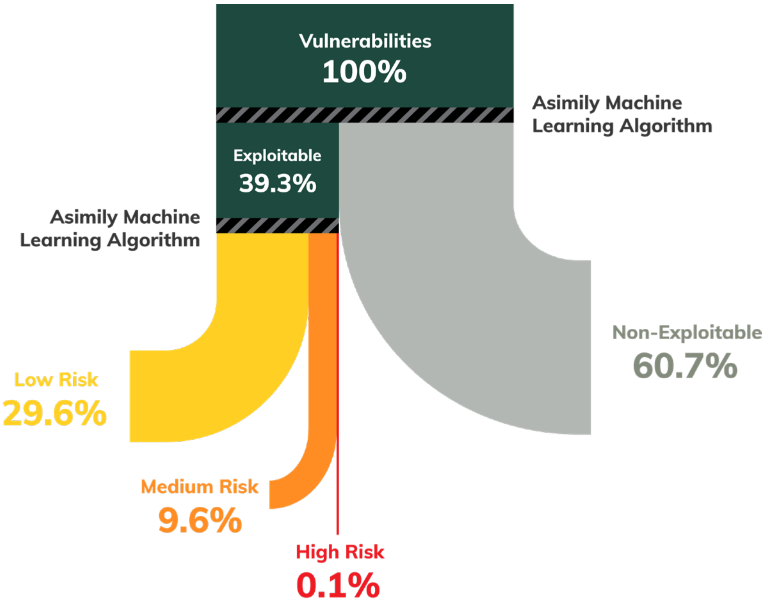
Routers

Security Cameras

Secure Your Connected IoT Devices and Reduce Vulnerabilities 10x Faster with Half the Resources

Asimily provides holistic context into an HDO's environment when calculating Likelihood-based risk scoring for devices. Our vulnerability scoring considers the compensating controls so you can more appropriately prioritize remediation activities.

HDOs efficiently identify high-risk vulnerabilities with our proprietary, patented algorithm that cross-references vast amounts of data from resources like EPSS, MDS2s, SBOMs, Common Vulnerability and Exposure (CVE) lists, the MITRE ATT&CK Framework, and NIST Guidelines.



Accurate Inventory & Unmatched Visibility

Harness Asimily's powerful protocol analyzer and deep packet inspection (DPI) to safely discover and automatically categorize your IoT assets, services, connections, and apps giving you the power to proactively manage risks, optimize resources, and fortify your security like never before.

Vulnerability Prioritization & Efficient Mitigation

Asimily's unique Impact, Likelihood and Utilization analyses show which vulnerabilities attackers will take advantage of in your environment. Allocate your resources to the riskiest devices first to promptly address vulnerabilities.

Threat Detection & Incident Response

Set device behavior rules that instantly identify any suspicious activities. Our engine swiftly spots deviations from normal behavior, ensuring that you can respond promptly to potential threats. Detect misconfigurations as well, keeping security posture high.

Risk Modeling & Simulations

Envision, predict, and act with unparalleled confidence, and unlock a new era of proactive risk mitigation. Calculate the least risk associated with a device before configuration and connection.

Connected Device Security, Reimagined

Securing the Internet of Things is far more complex than securing traditional IT equipment. Poor security practices at IoT and IoMT device manufacturers paired with minimal visibility by IT and security teams make connected equipment a major security risk. The distributed and broadly installed nature of these devices means that a risk-based approach is required. This can be done, and thankfully Asimily can help companies implement and manage a risk-focused method of securing IoT devices for a more secure future.

Asimily's IoMT and IoT Risk Management Platform

- Creates a complete IoT and IoMT inventory, collecting 100+ attributes for each device;
- Identifies and prioritizes the riskiest vulnerabilities;
- Recommends simple, validated mitigation actions;
- Conducts a full flow analysis for each device, recording all communication patterns across the network;
- Calculates risk for every connected device based on device attributes, dataflows, vulnerabilities, anomalies, configuration, and overall criticality of the device on operations;
- Generates ACLs for targeted segmentation for use by a NAC;
- Flags anomalous device behavior based on profiling data from millions of IoT devices;
- Makes it easy to set policies to monitor accepted risks and identify suspicious activity proactively;
- Automates packet capture for forensic analysis of any IoT device to support root cause analysis;
- Documents when the device is being used so users can understand utilization and operational efficiency;
- Allows device configuration snapshots to be taken, to thwart ransomware and simply recovery; and
- Risk simulator helps determine the benefit of work before it is performed, increasing team efficiency.

Asimily can help enterprise organizations drastically reduce cyber risk while minimizing resource and time costs.

To see how Asimily can help your organization, **arrange a demo today.**

About Asimily

Asimily is an industry-leading risk management platform that secures IoT devices for medical, diagnostic, life sciences, pharmaceutical, and enterprise companies.

Connect With Us

info@asimily.com
440 N Wolfe Road
Sunnyvale, CA 94085
(833) 274-6459
(833) ASI-MILY