The State of Cyber Asset Exposure Management in 2025

The Top Challenges in Hospital Cybersecurity

asimily

Survey Findings

Major Challenges that CISOs Want to Solve First 5

Biggest Device Risk Management Barrier 6

CISOs Rely on Disconnected Methods to Remediate Vulnerabilities in IoMT 8

Introduction

Cyber asset exposure management is one of the most persistent challenges facing hospital CISOs. The threat of unintentionally exposed assets, whether workstations, network gateways, or connected medical devices, creates the risk of enormous potential consequences.

If attackers can compromise the right asset and achieve lateral movement, there could be a major negative impact on patients and overall hospital operations.

The industry-wide shift towards cyber asset exposure management is fueled by a rising trend in cyberattacks targeting healthcare organizations. In fact, 93% of healthcare organizations experienced common cyberattacks in the past 12 months, according to Proofpoint and Ponemon Institute. The risk of a threat actor achieving initial entry and compromising critical patient data is very real. It becomes especially acute with greater usage of connected medical devices, also known as the Internet of Medical Things, becoming more integrated into the day-to-day operation of hospitals. CISOs need to manage hundreds of potential entry vectors, protecting their internet-connected infusion pumps, security cameras, IT workstations, tablets that doctors and nurses carry from room to room, and more.

Cyberattacks can cost up to $3.9 million for hospitals to recover from, according to Ponemon. That recovery number includes direct costs as well as lost revenue. It's incumbent on CISOs to protect their hospital infrastructure from compromise – not solely for lost revenue, but also to limit the interruptions to patient care and improve health outcomes.

The growing attack surface and exposure risk mean that hospital CISOs have to address many more possible entry points for attackers. With around 10 to 15 connected medical devices per bed in the average hospital, according to HIPAA Journal, this can mean upwards of 350,000 IoMT devices for hospital CISOs to protect. And not all of these devices are known or easily tracked throughout the hospital facility.

Data overload, internal process barriers, and more also frustrate the efforts of hospital CISOs to protect their critical infrastructure. Asimily surveyed dozens of hospital CISOs in an effort to better understand their challenges and the risks facing their infrastructure as it relates to IoMT systems.

According to the Ponemon Institute,

93% Of healthcare organizations experienced common cyberattacks in the past 12 months

$3.9M Healthcare organizations experience high costs of recovery from a cyberattack

10-15 Connected medical devices per bed in the average hospital

350K The average number of IoMT devices per hospital that CISOs must protect

This report will examine their challenges, the role of the CISO overall in hospitals, and provide actionable insights into resolving these issues in 2026.

Survey Methodology

With the help of the third-party survey platform SurveyMotion, Asimily surveyed dozens of North American Hospital CISOs about their challenges and their roles in their organizations. Asimily sought to uncover the major barriers beyond device visibility that CISOs and security teams must conquer.

Of the CISOs that Asimily surveyed,

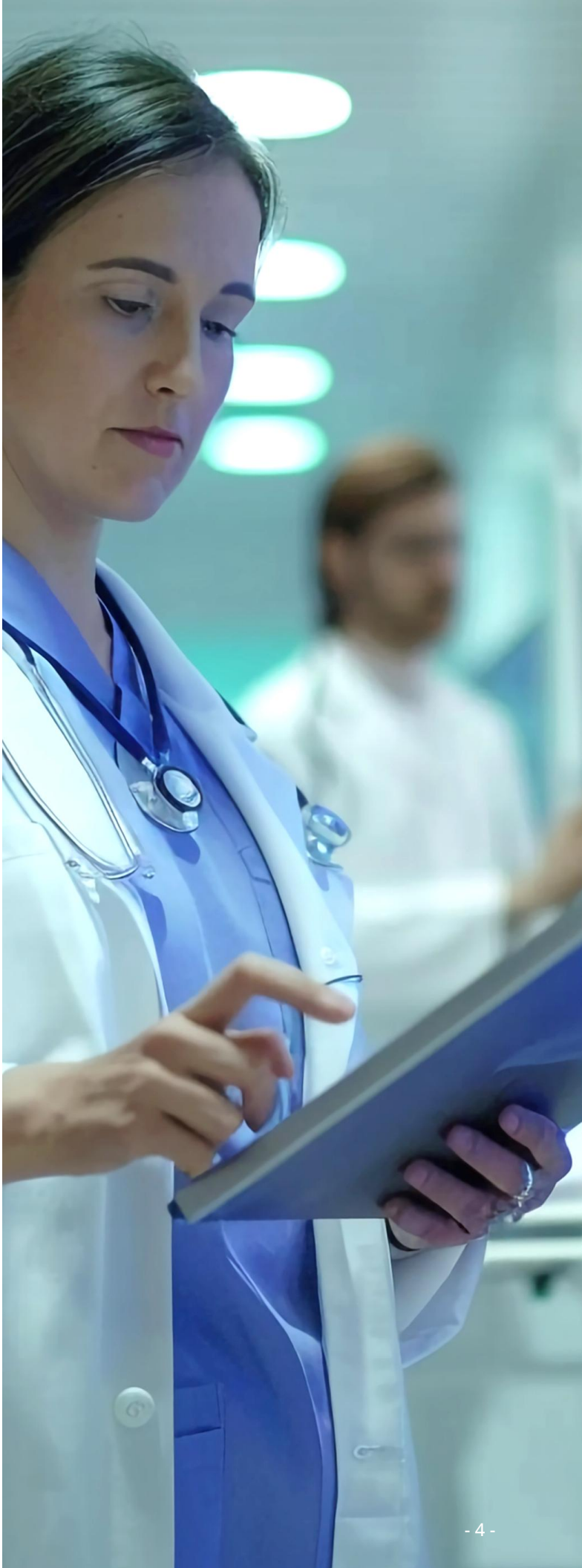
50% lead and make decisions about IoMT security in their organizations,

26% having influence over the decision but not final authority.

4% of CISOs have no direct role in security decision-making,

indicating that most hospital CISOs are well-enabled to direct the overall security posture of their organization's IoMT fleet.

Their insights indicate major trend shifts in how organizations manage exposure across all of their cyber assets – and what hospital CISOs can do to proactively address this challenge going forward.



CISO's Are Still Trying to Solve the Asset Visibility Challenge

Hospitals, on average, spend about **4% to 7% of their IT budget on cybersecurity**, according to CDW. The bulk of technology budgets in hospitals is allocated to improving patient care and patient outcomes, with security often seen as an afterthought. This budget has to be spent on protecting the entire infrastructure, and can sometimes pale in the face of spending on health technology related to patient care.

Only 4-7%

of a hospital's budget is being spent on cybersecurity

Source: CDW

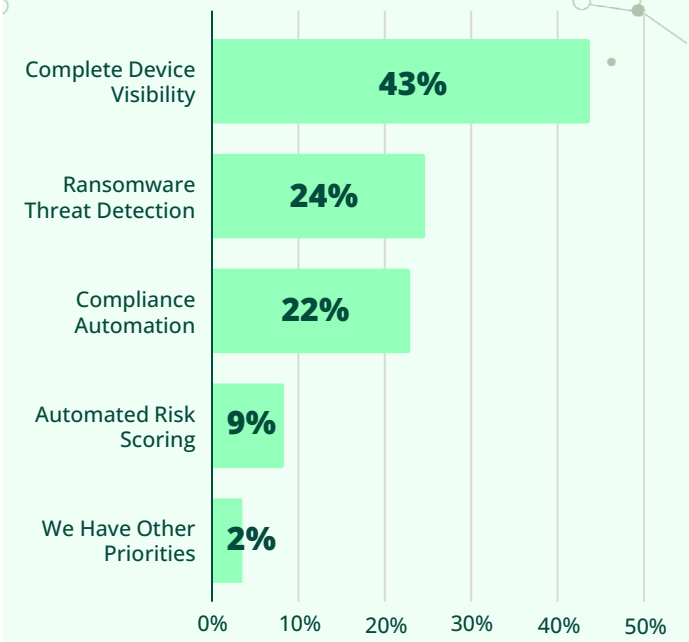
When it comes to defense, CISOs have to balance other teams' needs. Groups like clinical engineering, health technology management, and procurement also have roles in securing cyber assets, which makes protecting these systems a highly cross-functional activity in the average hospital; this can make it more challenging and vital to hospital security.

Part of understanding how to secure cyber assets within the hospital system lies in partnering with the teams who may be using these devices more directly on a day-to-day basis. Given that CISOs do have a strong role in most cases, this can be an easier negotiation, but it still needs to engage partner teams within the hospital.

There are also substantial challenges beyond organizational responsibility facing CISOs. Figure one below shows the four biggest barriers that CISOs would instantly solve as it relates to connected medical devices. Complete device visibility tops the list at 43%, indicating that CISOs need greater intelligence on the technologies connected to their network.

Visibility into the full cyber asset landscape has become table stakes in terms of protecting critical data. It's a major challenge for CISOs largely because many are now working without a holistic approach to visibility across IT, IoT, IoMT, and OT.

Figure 1: Major Challenges that CISOs Want to Solve First



Source: Asimily Survey Data

That's the core difference in why visibility is a challenge for cyber asset exposure management; trying to apply an integrated device protection model requires new intelligence. When platforms lack insight into the full scope of assets, then CISOs struggle to protect patient data and understand how attackers might compromise their systems.

Ransomware threat prevention landing at 24% also indicates the criticality of defending cyber assets and connected devices against compromise, but this practice can only be effective when all IoMT, OT, and IoT devices are fully discovered and visible.

The role of the CISO is clear in device security, especially in partnership with other groups in the organization. However, there remain barriers that go beyond visibility and threat detection. Understanding those risk management challenges is key.

Internal Process Issues Create the Biggest Barrier to Effective IoMT Device Risk Management

Securing IoMT devices is as much about risk management as it is about deploying security tools for monitoring. It's a well-known fact that IoMT devices are not often designed with security as a primary concern.

As a result, protecting connected devices from compromise is as much about risk management as it is about security best practices.

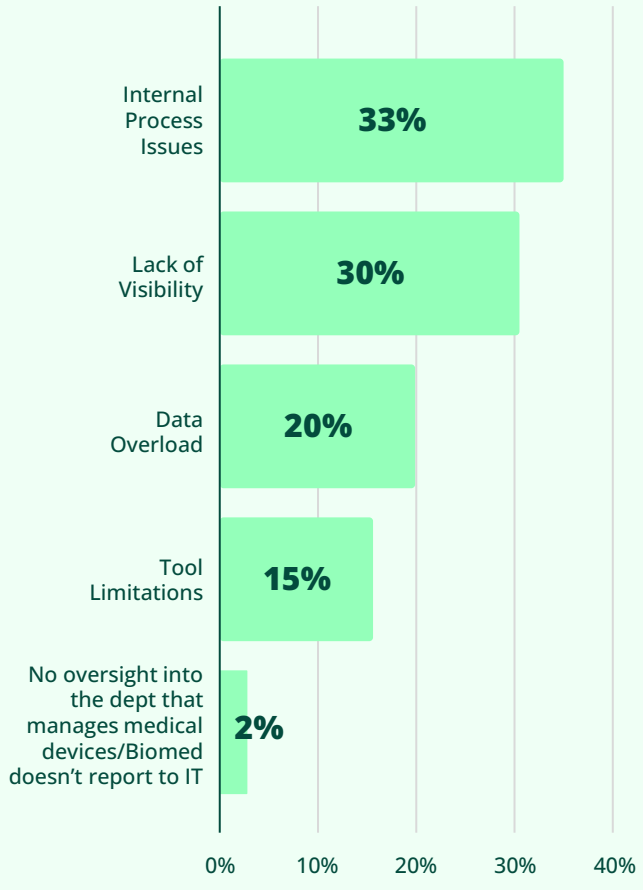
Asimily surveyed CISOs about the major barriers facing effective IoMT device risk management in their hospitals. Their responses are collected in Figure 2 below.

Internal Process Issues
(33%)

Internal process issues top the list at 33%, and are also the most generalized barrier to risk management. A process issue could be something as simple as ownership challenges, especially as it relates to device security. In many organizations, health technology management or clinical engineering might own the deployment or maintenance of medical devices. Meanwhile, security finds out after the fact when a new device is added to the network.

IoMT often has no clear owner within many hospitals. Instead, responsibility for the secure deployment and maintenance of the machinery gets passed around from department to department, without any direct lines of responsibility. Process issues can also relate to third-party technicians being called in to resolve problems without communicating any configuration changes they make. It can also lead to configuration drift, which may open up hospitals to potential compromise.

Figure 2: Biggest Device Risk Management Barrier



Source: Asimily Suvery Data

Lack of Visibility
(30%)

Lack of visibility into IoT, IT, OT, and IoMT equipment is only barely behind process issues as a major challenge, with 30% of CISOs marking this barrier as one of the most significant. Visibility should be table stakes for security professionals, but the reality is that companies are starting to look for a more holistic framing and have yet to achieve that.

Limited intelligence into what cyber assets are connected to the network creates major risks because CISOs don't know which systems they need to protect or where they are physically located. It's incredibly easy for HTM teams to set up a new device and connect it without informing security, or for a doctor or clinician to bring something from home, like a Bluetooth speaker, and link it into the hospital network.

Data Overload
(20%)

Data overload, at 20% of CISOs, likely relates to the sheer number of signals coming in from connected medical devices. As previously stated, the average hospital has 10 to 15 connected medical devices per patient bed. Larger facilities can easily have 350,000 IoMT systems sending network traffic across the hospital throughout the day.

That's a lot of signals flying through the network and communicating with each other. This level of information and data points easily overwhelms security teams, especially when they have to validate what is and isn't normal traffic from all those connected systems. Getting the right data in place and limiting the flow of signals into security dashboards can help make the flow of information more manageable.

Tool Limitations
(15%)

Tool limitations at 15% are a major barrier as well. CISOs need the right tools in place to be able to untangle all the data they're receiving from the network. Many security solutions designed to track signals from IoMT devices also don't ingest information from traditional IT like workstations and servers.

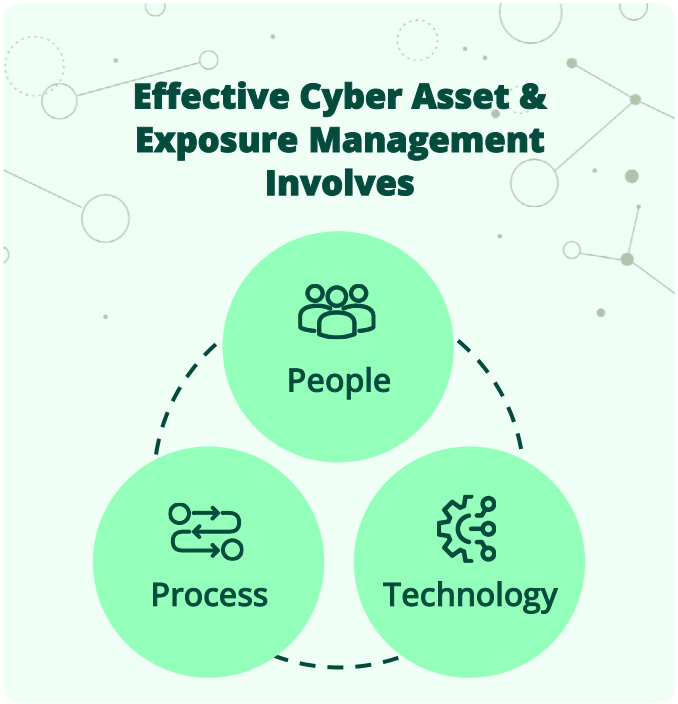
This limits comprehensive network visibility and makes it impossible to realistically prioritize risk. CISOs need the right tools in place to both accurately assess and even mitigate risk – without creating more noise.

Systems that don't unify data or can't easily understand all cyber assets on the network can create a false sense of security. What is needed is a single pane of glass into your organization's entire cyber asset fleet.

No Oversight Over Team
(2%)

The last major challenge at 2% is limited or no oversight over the team that manages technology. This barrier to risk management can produce issues related to configuration changes or drift, and technicians making changes to devices without security being aware of them. CISOs need some level of insight into changes being made throughout the network; otherwise, they risk security holes being opened without their knowledge.

This barrier is easily solved with deeper cooperation between teams or internal realignment to ensure that the technicians maintaining medical devices on the ground communicate changes back to a central security team. CISOs need to work with other stakeholders to determine what they're working on and how it impacts security.



How CISOs Manage Exposure Across All Cyber Assets

Vulnerabilities in IoMT devices present the most significant challenge that CISOs have to address in 2026 for effective exposure management. The problem is that security leaders often struggle to effectively remediate even identified vulnerabilities in connected medical devices. Manufacturers may limit the ability to deploy patches even when they're made available, forcing CISOs to hew toward mitigating risk rather than remediating vulnerabilities.

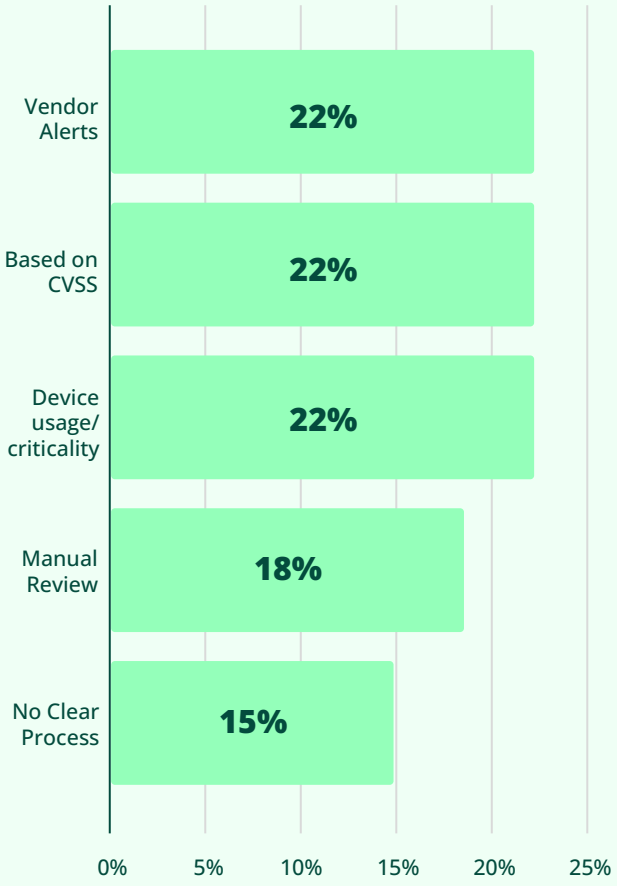
The most effective method of remediation relies on prioritizing vulnerabilities based on severity and impact to the organization. How CISOs arrive at their prioritized list of remediations can vary in terms of method, but they arrive at the same point of resolving the most impactful weaknesses in their specific network.

When Asimily surveyed CISOs on their prioritization methods for IoMT vulnerabilities, we found that 22% use a combination of vendor alerts, CVSS, and device usage or criticality as their criteria for deciding what vulnerabilities to remediate (Figure 3). 18% of CISOs use a manual review to prioritize vulnerabilities, while 15% lack a clear process for how to resolve issues in IoMT devices.

Manual Review = No Vulnerability Prioritization

Manually reviewing each of these disparate data sources creates a **significant challenge** for resource-constrained teams needing **to prioritize the riskiest and highest impact vulnerabilities** to remediate. Moreover, manual review often can't efficiently put the vulnerability in the broader context of your network and what sort of impact the issue can have. It's far more effective to use a comprehensive cyber asset and exposure management platform that identifies vulnerabilities, places them in the specific network context, and then CISOs can determine efficiently if an exploit is realistic or not.

Figure 3: CISOs Rely on Disconnected Methods to Remediate Vulnerabilities in IoMT



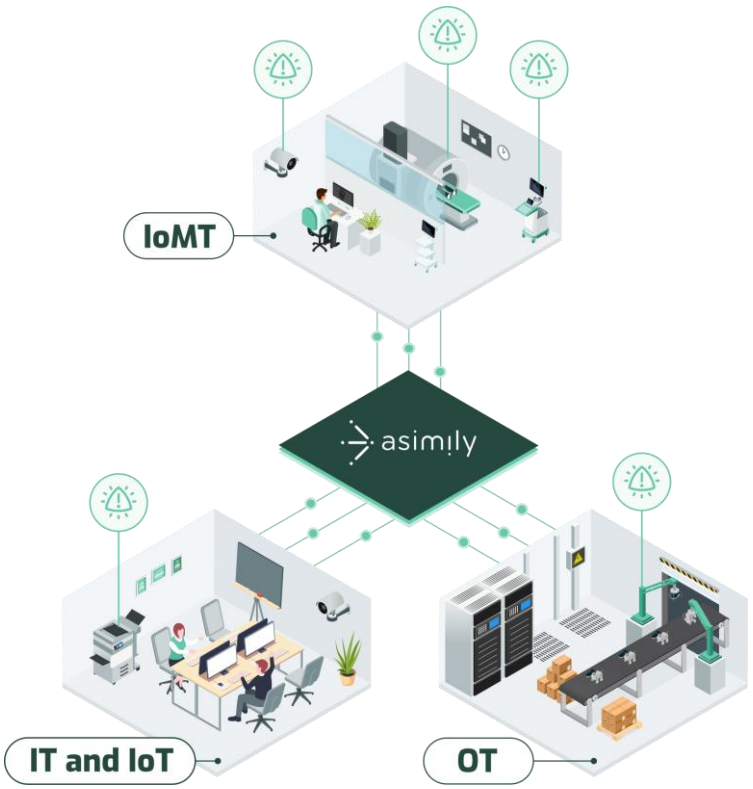
Source: Asimily Suvery Data

Vendor alerts and **CVSS** can be effective methods of **prioritizing vulnerabilities**, but the issue with vendor alerts is that they **may lag behind identified threats**. There is typically a "patient zero" when vendors send out alerts about vulnerabilities, and the risk there is that a hospital may have experienced a breach before the vendor notifies the rest of their customers about an issue. Basing remediation on CVSS provides severity scoring, but lacks the context of the individual hospital's network. A critical CVSS score may actually have no impact in a particular network if vulnerable systems are segmented and airgapped effectively.

Basing remediations around device usage and **criticality** is the **most effective method of vulnerability prioritization by far**. Vulnerabilities in an MRI machine or infusion pump might need to be prioritized above vulnerabilities in the marketing website or an administrative workstation, for example. This prioritization also needs to be based on whether an exploit could actually cause issues or not. If the hospital network is structured with effective segmentation or airgapping between critical systems, or access control is deployed efficiently, then even the most critical vulnerabilities may be mitigated with limited patching.

When CISOs leverage device criticality or usage metrics to decide which IoMT vulnerabilities to remediate, they can usually isolate **the top 1% riskiest devices, saving time while achieving better results.**

How Asimily Helps Hospital CISOs Resolve Their Cyber Asset Exposure Security Challenges



Asimily has built its cyber asset exposure management security platform around ensuring hospital CISOs can protect their network architecture effectively. With the ability to monitor network traffic for IT, IoT, IoMT, OT, and more, organizations that use Asimily gain critical intelligence into their actual device behavior and full network visibility.

The Asimily platform scans networks to build device inventories for unparalleled visibility into the IT, IoMT, IoT, and OT systems attached to hospital networks and the communication pathways between them. This ensures insight into what the actual cyber asset landscape looks like and where the risks may be for hospital CISOs seeking to limit the possibility of a breach.

With Asimily, Healthcare CISOs Can:

- Gain a complete repository of IT, IoT, OT, and IoMT devices while finding "unmanaged" devices with the combination of Asimily's protocol analyzer, deep packet inspection (DPI), and AI/ML-based traffic analysis.
- Protect devices during data gathering by using any of passive, protocol-based, API-based, or combinations, including via integrations.
- Enrich device data with details such as manufacturer, configuration, device type, IP addresses, applications, OS, and software versions to provide a comprehensive inventory record for each asset.
- Segment, microsegment, or apply targeted segmentation to their network using Asimily's recommendations to secure their critical assets and reduce the blast radius should an attack occur.

Asimily also integrates threat detection and response capabilities, empowering teams with anomalous behavior monitoring and device rules that can capture potential threats. CISOs can use this capability to determine where there may be active attacks and respond to them quickly and efficiently. With this functionality, Asimily ensures that teams have network context and understand normal device behavior, so their limited time is spent effectively.

Asimily also empowers effective governance, risk, and compliance (GRC) strategies for IoT and IoMT devices. Using risk modeling and device hardening guidance, security teams can determine potential risks prior to device purchase or even during the process of implementation by other groups. They can also leverage Asimily's GRC functionality to define specific policies and alerting on configuration drift, limiting the risk of changes from third-party technicians or other groups within the hospital.

With Asimily, hospital CISOs can protect their critical technologies and ensure that clinical teams can focus their attention on patient care. Not whether they have secure technologies.

A Secure Future for Hospital Cyber Assets

Cyber asset exposure management is incredibly complex for hospital CISOs. They have to contend with limited visibility into devices installed on the network, process challenges internally, and data overload, among other lingering issues that stymie the efforts of security teams. Resolving these challenges requires a platform approach that unifies signals from IT, IoT, IoMT, and OT systems for comprehensive intelligence into potential exposures through the network.

The problem of cyber asset exposure management is so broad and complex that there needs to be a single, unified view that brings together all device information alongside partner solutions like vulnerability management, anomalous behavior monitoring, and more.

Ultimately, security teams and CISOs need a comprehensive approach to IoMT security that includes **a solution like Asimily** with the **ability to unify data between IT and IoMT systems** and **provide comprehensive insight into the full asset inventory**. Only then can hospital CISOs effectively manage their cyber asset exposure risk and protect patient data now and in the future.

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

About Asimily

Asimily is the next-generation cyber asset and exposure management platform. Asimily's comprehensive platform enables best-in-class exposure management across IT, IoT, OT, and IoMT – empowering your teams to reduce risk efficiently

info@asimily.com
1-833-274-6459
Sunnyvale, CA USA