Cynerio

White Paper

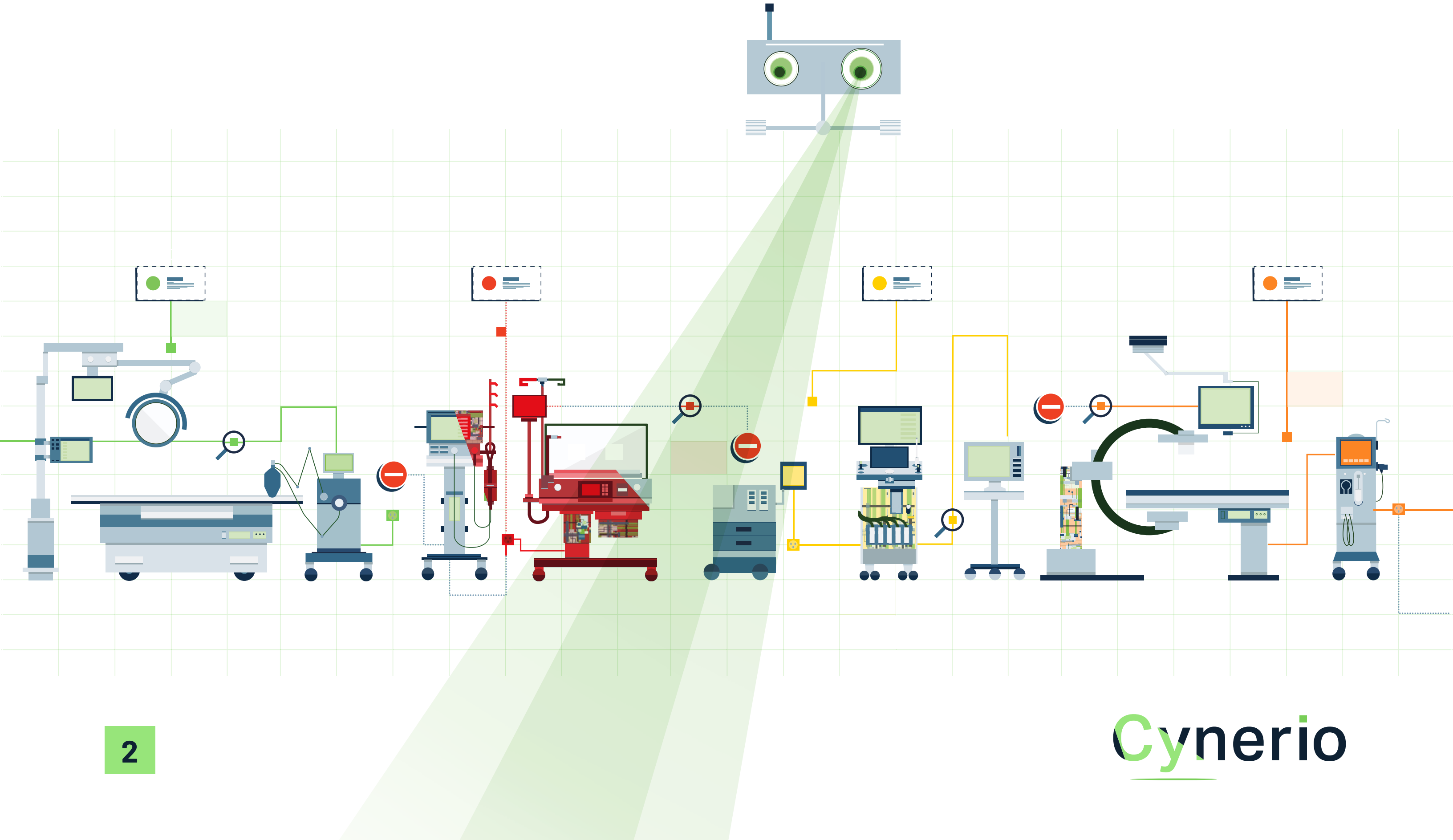
Extending Medical Device Cybersecurity Building On Existing Technology To Address Risk

Executive Summary

Healthcare organizations have unique cybersecurity challenges. Cyber criminals have steadily ramped up their attacks on the sector for the past several years, with devastating ransomware events becoming commonplace. While often presented by industry members in a victimized manner, the focus of cyberattacks on healthcare is actually quite simple to explain. In short, hospitals have traditionally adopted new technologies while underinvesting in sufficient cybersecurity protections. In the event of an attack it is common to pay a high ransom in short order, further encouraging future attacks.

Healthcare isn't a primary focus of cyber criminals because they're evil. It's their primary focus because it's profitable.

With these challenges, there is one fortunate situation often overlooked - the foundation for medical device security is already in place at most institutions. As a result, hospitals can improve device security by simply extending their existing technology, educating their people, and introducing cybersecurity best practices to the organization. By automating inventory and visibility, building on existing processes and technologies, prioritizing vulnerability remediation, and ensuring that basic cyber hygiene is in place, organizations can greatly reduce the risks posed by their growing inventory of medical devices.



Confronting Many Barriers Amid Increasing Risk

Medical devices have been called "the next disruptor in healthcare"[1]—for good reason. The market sometimes known as the "internet of medical things" (IoMT) grew from $41 billion in 2017 to $158 billion in 2022[2]—a trendline that is expected to continue for at least the next five years[3]. For healthcare organizations, the result is steady increases each year in both the device count and the number of unique device types. Today, a typical 500-bed hospital might have as many as 7,500 devices[4].

Beyond the management challenges posed by their growing numbers, medical devices pose significant cybersecurity risk for hospitals. One recent study found that 20% of healthcare ransomware attacks began with an attack on a medical device[5]. Another found that ransomware attacks in healthcare increased by an astounding 94% over a one-year period[6].

Putting these two statistics together, we estimate that the raw number of successful attacks launched through a medical device nearly doubled in the space of 12 months and is likely continuing to rise. This is not surprising given that according to Cynerio research, 53% of connected devices contain critical risks to data confidentiality, service availability, or patient safety[7]. In a large hospital, that can translate to several thousand devices that pose risk to the institution every time they are used.

It is impossible to know all the reasons that hospitals are sustaining so many attacks, but some of the factors are obvious. Hospital employees continue to work under heavy stress as waves of COVID-19 continue, and this may make them susceptible to accidentally clicking on just one of the billions of phishing emails sent out each year. And cyber criminals know that they have more leverage over hospitals than nearly any other organization to which they could deliver ransomware, as getting systems back online is measured not just in financial terms, but also in impact to patient care.

[1] **"Life-Changing Medical Devices: The Next Disruptor in Healthcare,"** Modern Healthcare, January 3, 2019

[2] **"IoT Healthcare in 2022: Companies, Medical Devices, and Use Cases,"** Insider Intelligence, April 15, 2022.

[3] **"Connected Medical Device Market Size Report 2022 Analysis Report by Industry Segmentation, Region, Manufactures, Cost Structure and Forecast to 2026,"** MarketWatch, May 11, 2022.

[4] Mike Milliard, **"Cybersecurity Pro: Networked Medical Devices Pose Huge Risks to Patient Safety,"** Healthcare IT News, February 29, 2016.

[5] **"The Impact of Ransomware on Healthcare During COVID-19 and Beyond,"** Ponemon Institute and Censinet, accessed May 28, 2022.

[6] Shwan Dickerson, **"Why Is Healthcare a Top Target for Cybersecurity Threats?"** Security Magazine, September 13, 2022.

[7] **"The State of Healthcare IoT Device Security 2022,"** Cynerio, January 19, 2022.

Industry Barriers to Healthcare Cybersecurity

Given the increasing risks, why do hospitals not simply lock down their devices from a security perspective? As is typical with this type of question, the answer starts with “it depends”. Healthcare organizations have several unique systemic problems when it comes to the broader topic of cybersecurity protection:

- **Historical underinvestment in cybersecurity.** Over the years, many healthcare institutions have fallen behind many other industries when it comes to cybersecurity investment. Even more recently, a 2021 survey found that just 11% of hospital IT professionals said that cybersecurity is a high priority for spending[8].

  There are undoubtedly multiple reasons for this, but the laudable goal of reserving as much budget as possible for patient care may be a factor. What organizations sometimes fail to realize is that cybersecurity investments can have a direct impact on patient care. This is nowhere more apparent than with medical devices, which may be attached directly to patients when an attack occurs.

- **The “wall of shame.”** The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 provided funding to kickstart the use of electronic health records across the U.S. medical system. The law also includes additional security standards for protected health information (PHI) beyond what is included in the Health Insurance Portability and Accountability Act (HIPAA), and it requires all institutions to report all data breaches affecting more than 500 patients to the Department of Health and Human Services (HHS). HHS, in turn, posts this information on a website informally known as the “wall of shame.”

  While HIPAA and HITECH have motivated hospitals to take steps to protect PHI, over-emphasis on finding quick fixes for compliance can result in underinvestment in a more holistic, comprehensive security strategy—which would also support compliance. Another unintended consequence of the “wall of shame” is that while it appropriately keeps consumers informed about data breaches, it also provides valuable intelligence to cyber criminals attempting further attacks.

- **The recovery conundrum.** When a ransomware attack occurs, the Federal Bureau of Investigation (FBI) advises all organizations to refuse to pay the demanded ransom. Of course, it would be good for society if no one paid, because cyber criminals would quit using the tactic if it were not successful in bringing them revenue. But many organizations do not see this as a viable option- especially hospitals. In 2021, healthcare organizations paid the ransom in 61% of successful ransomware attacks- more than any other industry[9]. It is not hard to understand why. First, losing all IT systems can have a tragic impact on patient care in the short term, and paying the ransom is by far the fastest way to restore systems. Second, it usually costs much less to pay the ransom than to restore systems in other ways- a process that could also leave the hospital crippled for weeks.

[8] Sebastian Klovig Skelton, **“Hospitals See Cyber Security Investment as a Low Priority,”** Computer Weekly, August 13, 2021.

[9] Kari Paul, **“Lives Are at Stake’: Hacking of U.S. Hospitals Highlights Deadly Risk of Ransomware,”** The Guardian, July 14, 2022.

The bottom line is that ransomware will be a profitable business model for cyber criminals as long as they can launch successful attacks. In the same vein, hospitals must learn to consider avenues to damaging this profitable business model, often by improving defenses, reducing attack impacts and ultimately destroying paths to revenue. To do so, hospitals will need to marshal their entire cybersecurity infrastructure in a strategic way to combat attacks across the entire attack surface-including medical devices.

Institutional Barriers to Device Security

Beyond systemic cybersecurity problems and issues inherent in the devices themselves, many institutions currently are experiencing several other barriers to adequate security for medical devices:

- **Ambiguity of roles.** Across the healthcare industry there is no clearly defined ownership of medical device security. While often assumed to be the responsibility of IT, Network or Healthcare Technology Management (HTM) teams, a recent Ponemon Institute and Cynerio survey found the ultimate ownership is even more widespread. From Operations Leadership (14%) to Users of Medical Devices (9%) and even COO/CEOs (2%), this study found no consistent ownership - a rarity for an industry that often prides itself on clearly defined responsibilities[10]. Recent efforts to shift responsibility to Chief Information Security Officers (CISO) are a step in the right direction, but are often complicated by ridgid organizational structures and unacknowledged levels of urgency.

- **Inadequate staff.** Even if each team's role is clarified, many organizations lack adequate staff to stay on top of device security. Staffing shortages currently affect organizations across the economy, but healthcare has special challenges. Many hospitals have critical shortages of nurses and other clinical professionals, exacerbated by a fluctuating patient census caused by the ebb and flow of COVID-19 variants[11]. The economics of this phenomenon makes it difficult to make new hires on the non-clinical side of the organization. And even if funds for new headcount are available, a worsening cybersecurity skills shortage impacts this function in all industries[12].

- **Insufficient funding.** Every team at every company wishes it had more budget, but healthcare economics in the U.S. are notoriously fragile. After hospitals endured more than two years of chaotic financials due to the pandemic, federal relief funds that were a critical lifeline are now expiring—even as a new variant of COVID-19 is filling hospitals again[13]. This may mean less money for just about every aspect of an institution's operations, including medical device management and cybersecurity.

[10] **"The State of Healthcare IoT Device Security 2022,"** Ponemon Institute and Cynerio, August 3, 2022.

[11] Christine Chung, **"As U.S. COVID Hospitalizations Climb, a Chronic Nursing Shortage Is Worsening,"** The New York Times, July 15, 2022.

[12] James Coker, **"Cybersecurity Workforce Gap Grows by 26% in 2022,"** InfoSecurity, October 20, 2022.

[13] Krista Mahr, **"Hospitals Struggle with Staff Shortages as Federal COVID Funds Run Out,"** Politico, July 25, 2022.

Device-Level Security Barriers

In addition to these systemic challenges, hospitals must cope with the unique challenges inherent in the devices themselves. In a nutshell, most were not designed with a level of security that users and patients often assume. Among the core challenges to securing devices are:

- **Long life cycles.** Medical device manufacturers rarely benefit from the planned obsolescence mindset that drives other industries. Whereas a cell phone is often upgraded every two years, medical devices are frequently in use for over a decade, typically much longer than manufacturers provide security, support and upgrades to protect patients. The industry's overwhelming focus on care often results in choosing between device functionality or security, with functionality consistently winning.

- **Component complexity.** While devices frequently have one core functional goal, the complexity in achieving that goal often requires dozens of components. From plastic outer shells to microprocessors, touch screens to electrical plugs, and customized operating systems to undocumented software, each layer of complexity introduces additional opportunities to identify an attack vector. Cynerio research has found that 53% of all IoT and IoMT devices at hospitals contain vulnerabilities that pose critical risks to patient safety, data confidentiality, or service availability[14].

- **Deployment insecurity.** Patient protection does not stop at securing the devices treating the patient. Updated, patched and otherwise secure devices can still introduce risk if improperly deployed within a hospital. Seemingly innocuous devices such as medical robots used to collect and deliver linens can become remotely controlled chunks of mobile metal if accidentally made accessible to the outside world[15].

The number, type, and nature of medical device vulnerabilities is only as complete as the most skilled cyber attacker's evil ingenuity on a particular day. One indication of the seriousness of this risk is an industry alert issued by the Federal Bureau of Investigation (FBI) in September 2022[16]. Citing Cynerio research and other sources, the alert recommends quick action toward a holistic cybersecurity strategy to protect connected devices.

[14] **"The State of Healthcare IoT Device Security 2022,"** Cynerio, January 19, 2022.

[15] **"JekyllBot:5 Vulnerability Disclosure Report,"** Cynerio, April 12, 2022

[16] **"Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities,"** Federal Bureau of Investigation, September 12, 2022

Extending Device Security, Not Cybersecurity Costs

The traditional answer to all of your cybersecurity problems is “resources”, but in healthcare additional spend on people, time and money takes away from care, recovery and livelihood. Luckily, the answers to all of your device cybersecurity problems need not be “money”.

Industry Challenges

- **Challenge: Historical underinvestment in cybersecurity**
  Opportunity: Getting on top of inventory and visibility.
  Of course, to secure a device, an organization must know that it exists and see where it interacts with the network. Unfortunately, many hospitals still have not completed the basic step of delivering an accurate, up-to-date inventory of their medical devices.

  Because the inventory constantly evolves, it is not sufficient to create a manually-populated spreadsheet—or even to manually enter data into a computerized maintenance management system (CMMS). The only way to have a point-in-time view of the entire inventory is to automate the process through continual scanning of the network to discern what is connected, and where. This gives a hospital visibility into not only what is connected, but also where each device is located. While inventory and visibility are absolutely necessary first steps, institutions should not mistakenly believe that the job of securing devices is finished when all devices are visible. Visibility does not secure devices; it simply makes it possible to secure them.

- **Challenge: The “wall of shame”.**
  Opportunity: Extending ePHI protections.
  Healthcare environments have long equated cybersecurity best practices with protecting patient data. While data protection is a key component of these efforts, it is neither sufficient, nor is it well executed in many environments. In most cases the in-place systems and processes used to identify and secure patient data have not kept up with the adoption of new systems. The result is a reliable annual increase in number of providers breached, total records exposed and fines levied despite incredible annual investment on patient protection. Healthcare leaders must challenge their current security providers to introduce and investigate emerging approaches to protecting patient data. Systems focused on identifying and securing medical devices should be evaluated based on their ability to identify points of exposed data that traditional systems may miss.

- **Challenge: The recovery conundrum.**
  Opportunity: Reevaluate ransomware response strategy.
  Law enforcement guidance is clear. Paying a ransom to recover a healthcare system will only provide more attacker motivation. Unfortunately, ransom payments are often the most affordable and immediate resolution to an attack, with a reported 47% of healthcare organizations paying a demanded ransom[17].

[17] **“The Insecurity of Connected Devices in Healthcare 2022,”** Ponemon Institute and Cynerio, August 3, 2022.

While paying a ransom is never recommended, doing so is understandable. In closed groups the recommendation of "Never pay the ransom, but always be prepared to" is freely shared and embraced. If this is an approach you are considering, further explore the mechanics of what will occur during a ransomware attack with your cybersecurity insurance provider. Who will negotiate? Where will the BitCoin be drawn from? What are your legal liabilities?

To be clear, paying a ransom is not an endorsed approach, but it is an understandable one. While improving your device security practices also consider the above factors and beginning theoretical ransom payment discussions with your insurance providers.

Institutional Challenges

When thinking about how to go about improving device security, organizations should consider several aspects of device security:

- **Challenge: Ambiguity of roles.**
  Opportunity: Determine organizational device security model.
  As noted, ownership of device security at some hospitals is in transition to security teams under the supervision of a CISO, while other organizations continue to house this function in one of many other teams. Hospitals are diverse, and there is no single approach that is best for all. Regardless of the ownership and organizational structure in place, almost all hospitals have the key components to improve their device security strategy. However, it is important that roles are clarified in advance, to ensure that the two groups are not unknowingly working in parallel—or worse yet, at cross purposes.

  1. **BioMed-led efforts** are spearheaded by HTM team members who have intimate familiarity with the devices themselves and how they interact with the network. Security team members can consult with the team on cybersecurity best practices and technology support.

  2. **Security-led efforts** are directed by the team with the most familiarity with the cybersecurity architecture, and these professionals can consult with the HTM team on device specifics.

  3. **Joint efforts** between the two teams can be very effective at many organizations. A cross-functional team can meet regularly during the rollout, and periodically afterward, to assess the program from network, security, and operational perspectives. One consideration in deciding on this option is where the HTM team sits in the organizational chart. Is it a part of the CIO's team, or is it a standalone department?

- **Challenge: Inadequate staff.**
  Opportunity: Build on existing processes.
  Rather than disrupting operations to launch a huge new device security program, organizations can easily attach security components to existing processes—new device setup, maintenance of existing devices, and updates to networking infrastructure. For example, it is significantly more efficient to patch devices in batch efforts during setup and routine maintenance than to reactively address time sensitive issues. More broadly, it is far more efficient to segment a network and properly onboard devices than to launch inherently insecure devices into a flat network, a combination known to exacerbate most healthcare cyber attacks.

- **Challenge: Insufficient funding.**
  Opportunity: Building on existing CMMS technology.
  Almost every hospital has a CMMS system, but few are using it to its full potential—and such tools provide a foundation for growth when it comes to medical device security.

  When an inventory and visibility tool is integrated with an existing CMMS, the two solutions work together to automate inventory, enhance data, provide workflow functionality, and provide a holistic view of the inventory from a single pane of glass. When risk reduction and incident response solutions are added, organizations can work through the CMMS to prioritize and execute on.

Device-Level Challenges

- **Challenge: Long life cycles.**
  Opportunity: Mitigating risk with informed prioritization.
  Hospitals need two kinds of information about each known vulnerability found in a medical device. The Common Vulnerability Scoring System (CVSS) measures the severity of each vulnerability, while the Exploit Prediction Scoring System (EPSS) measures the likelihood of a vulnerability being exploited. Both measures are critical to effective prioritization of remediation, as a vulnerability that has almost no likelihood of being exploited is a low-priority fix, regardless of severity. Risk reduction tools that take both scores into account enable hospitals to systematically and effectively reduce risk.

- **Challenge: Component complexity.**
  Opportunity: Extending beyond the CMMS.
  While an existing CMMS is an excellent foundation for device security, it is not a magic bullet that solves all problems. Many institutions will benefit from seeking out expertise from other resources, such as the in-house or outsourced security operations center (SOC), a managed security services provider (MSSP), providers of device security technology solutions, and experts from other industries who can bring a fresh set of eyes to the challenges faced in healthcare.

- **Challenge: Deployment insecurity.**
  Opportunity: Integrating cybersecurity best practices.
  One of the best ways to protect medical devices is to align security practices with the best practices that are likely already being practiced in other parts of the network. There are any number of guides and checklists that can help institutions confirm that their processes are adequate[18].

  In this sense healthcare has a notable advantage to rapidly improving security posture that other industries did not - the guidance is often available and well known! Many of the steps needed to secure a hospital (efficient device patching, microsegmentation, incident detection, etc) have been developed and perfected by the financial, insurance and commercial industries over the last decade. Adopting these proven approaches will help avoid the time, effort and investments already invested by more forward thinking industries.

[18] For example, see Susan Kelly, **"8 Ways Hospitals Can Prevent a Cyberattack,"** HealthcareDive, November 1, 2022.

Holistic Security for Diverse Devices

Medical devices are unique. Unlike desktops, laptops, and other endpoints that an organization might manage, there are hundreds of distinct device types made by dozens of manufacturers at every hospital. And unlike the IoT devices used by other organizations, medical devices provide direct, often life-or-death, patient care. Each software vulnerability on a medical device carries the potential for a devastating attack—and a grave threat to patient safety. And a steadily increasing volume of attacks on healthcare organizations makes the security of these devices even more urgent.

The good news is that most hospitals already have the foundation in place to mitigate the risk posed by these devices. The security team already has tools and processes in place, many of which simply need to be extended to the device inventory. The HTM team already has a cadence of device maintenance that can simply be retrofitted with security practices. And the hospital likely already has a CMMS tool that can form the foundation of an automated inventory and visibility system, as well as a prioritized risk reduction program.

With a little strategic thinking, organizations can greatly reduce the risk of medical device attacks while minimizing cost and utilizing existing team members. The result will be much lower risk to service availability, data integrity, and patient safety.

Extending Healthcare Cybersecurity with Cynerio

Cynerio was founded in 2018 with one goal in mind: to secure every IoT, IoMT and OT device in healthcare environments. At the core of our capabilities is the Cynerio Collector, a physical appliance that uses Deep Packet Inspection (DPI) to analyze devices, network traffic and malicious activity while protecting patient data. From improving device-level patch management to enabling adoption of microsegmentation strategies long ago embraced by other industries, Cynerio combines proven security approaches with healthcare-specific innovation that enables improved hospital cybersecurity practices despite tight budgets and increasing cyberattacks.

Cynerio provides the combination of reactive and proactive measures needed to prevent common healthcare-focused attacks and respond within minutes to those that are not prevented. Among Cynerio Offerings are:

Attack Detection & Response. Developed in conjunction with healthcare organizations experiencing cyberattacks despite comprehensive adoption of best in breed cybersecurity technologies, Attack Detection and Response provides day 1 protection and addresses active attacks frequently missed by traditional systems. Backed by the Cynerio Live research team, all identified risks are fully researched and validated before alerting customers with detailed data regarding the attack and clear, actionable guidance on immediately addressing all areas of compromise. Attack Detection & Response customers often measure success in addressing attacks in minutes and hours rather than months and dollars. To learn more about Attack Detection and Response visit Cynerio.com.

Preventative Risk Management. Developed originally as a deeply technical microsegmentation engine, Cynerio's Preventative Risk Management offering has evolved into the industry leading technology for proactive defense of devices in healthcare networks. From infusion pumps and CT machines to SmartTVs and Teslas, Preventative Risk Management identifies all devices on a network, analyzes them for known security issues and provides clear, actionable guidance on addressing those issues. Beyond the core device-focused analysis, network traffic will be analyzed, policies generated and tested, and vendor access controls enabled along with a variety of additional capabilities that will scale preventative cybersecurity practices without requiring unachievable levels of investment or time. To learn more about Preventative Risk Management visit Cynerio.com.

Cynerio 360 Platform. Regardless of security goals, a combination of proactive and reactive approaches is always a requirement. The Cynerio 360 Platform provides a single pane of glass for all Cynerio findings with prioritized, actionable guidance on how to reduce risk without breaking the bank. Learn more about Cynerio's full suite of products at Cynerio.com.

Technical Account Managers. The cybersecurity skills shortage has had a particularly negative impact on hospitals who are often unable to find and retain top level talent. Cynerio Technical Account Managers (TAM) ease the pain of this skill shortage by providing support and guidance at the industry, institutional and device levels. Dedicated TAMs ensure successful deployment, adoption and long-term success of Cynerio engagements, resulting in improved security practices and safer patients. Learn more about TAMs at https://www.cynerio.com/services/technical-account-manager.

Cynerio Live. A core component of all security innovation is cutting edge research that identifies and guides improvements related to new security vulnerabilities. The Cynerio Live research team not only performs research that leads to improved product offerings, but is also available to Cynerio customers on an as-needed basis. From explaining the newest vulnerabilities discovered in the wild to leading response during an active cyberattack, Cynerio Live provides expertise when it is most needed by hospitals. Learn more about Cynerio Live at Cynerio.com.

Cynerio has one simple goal - to secure every IoT, IoMT and IT device in healthcare environments.

Learn how at www.cynerio.com.

Cynerio

Healthcare IoT Cybersecurity

Securing What Others Only See

www.cynerio.com