Implementing a Strong IoMT Security Posture

Implementing a Strong IoMT Security Posture

Introduction

In the rapidly evolving ecosystem of digitized healthcare, IoMT (Internet of Medical Things) technologies have become an irreplaceable component of patient care. With IoMT-based devices, physicians and patients can monitor conditions in real-time, allowing for maximum disease management and enhanced patient care outcomes.

The benefits of IoMT are so appealing that the IoMT market is expected to reach a valuation of $158 billion by 2022.[1] By 2023, it is expected that 68% of devices in hospitals will be connected.[2] However, despite its advantages, IoMT puts healthcare organizations and lives at risk. Because healthcare groups often lack knowledge of their connected inventory, own a wide variety of devices, and purchase products that aren't secure by design, cyberattacks remain a pervasive threat.

In this paper, we will discuss how discovery and visibility, policy management, and enforcement represent a starting point for improved healthcare.

---

[1] "The Internet of Medical Things Moment is Here," World Economic Forum, Kayla Matthews, May 10th, 2019

[2] "Eight IoT Barriers for Connected Medical Devices and How to Overcome Them, Deloitte, 14 Aug, 2018

Discovery and Visibility

In order for healthcare organizations to provide seamless patient care, identifying and monitoring IoMT inventory is essential. Administrative managers should know the vendor, model, serial number, and operating system of each and every connected device. This information can be invaluable in quickly removing devices that have been recalled for safety reasons, in minimizing overhead costs, and in reducing overall risk.

From 2015 and 2019, the US Food and Drug Administration (FDA) issued more than 100 medical device safety warnings or recalls, including a handful in regards to cyber security concerns.

In early 2020, the FDA issued a Class 1 recall of 774,000 infusion pumps sold in the United States due to software errors and potential vulnerabilities.[3] The recall only pertained to specific model codes and lot numbers, and organizations were advised to then wait for the manufacturer to reach out about a software update. Until the software update is released, devices "remain vulnerable," says the FDA.[4]

When instances like these occur, healthcare providers, distributors and facilities need to quickly isolate and remove devices from their inventory. Accomplishing this type of task without a discovery and visibility tool is overwhelming.

The FDA issued a Class 1 recall of 774,000 infusion pumps due to security threats and vulnerabilities.

In addition to taking precautions in regards to external threat warnings, hospitals and healthcare groups must also take precautions when it comes to internal threats. As a medical provider group, you know that lost and stolen equipment costs US hospitals millions of dollars, annually. In 2020, a hospital employee faced federal charges for the theft of five ventilator machines [5], which collectively may have cost the hospital as much as $175,000.[6] By avoiding inventory depletion when it comes to devices, you can remain aligned with group buying contracts, avoid paying higher prices for additional equipment, and ensure continuous patient care.

For these reasons and more, investing in automatic discovery and visibility for your IoMT systems can facilitate smooth day-to-day operations, and reduce overall risk.

In 2020, a hospital employee faced federal charges for the theft of five ventilator machines, which collectively may have cost the hospital as much as $175,000.

[3] "Thousands of Infusion Pumps Recalled After Several Injuries and a Death," Drugwatch, Michelle Llamas, 3 Aug, 2020
[4] Recalled Product, FDA, 6 March, 2020
[5] "Worker stole ventilators, Covid-19 supplies from VA center to sell on eBay, feds say," The News Tribune, Summer Lin, 18 June, 2020
[6] "States reportedly fend for themselves with inflated ventilator prices," Mass Device, Sean Whooley, 15 June, 2020

Policy Management

With over 4 million IoMT devices worldwide, a broad range of device types, and a range of data repositories, hospitals and healthcare systems contend with a dizzying array of endpoints to secure.[7]

The global healthcare sector reports that nearly 187 million cyber threats are directed towards web-based scheduling applications per month. This shakes out to about 498 attacks per organization.[8] Under-secured, unknown and unmanaged endpoints are particularly problematic, as cyberattacks typically exploit neglected elements within a system's configuration.

Several years ago, blood gas analyzers belonging to three different US hospitals were the source of malware threats. The devices were found to contain vulnerabilities that enabled hackers to access and move around the larger network. As a result, an untold volume of patient records were compromised and exfiltrated to Europe. These endpoint threats could have been managed effectively, but were overlooked.[9]

Policy management helps you see your blind spots. With a unified policy management tool, you can secure all of your infrastructure's diverse components.

The global healthcare sector reports that nearly 187 million cyber threats are directed towards web-based scheduling applications per month.

The best policy management tools enable you to set uniform policies for the entire infrastructure with a combination of auto-generated policies and user generated policies. Dynamic, customizable and granular policy management minimizes your endpoint risk.

Enforcement

While hospital and healthcare systems strive to purchase devices that are secure by design, many continue to rely on entire fleets of legacy devices that lack built-in security or that contain unknown vulnerabilities.

For example, in the early spring of 2019, the US Food and Drug Administration (FDA) discovered that certain implantable cardiac devices, related clinical apparatuses, and home monitors could be hacked. Specifically, the devices lacked communication encryption, authentication, or authorization protocols to preventdata interception.[8] Ostensibly, a hacker could intercept patient data in transit, and precipitate a range of consequences.

With devices that are not secure by design, unauthorized users may be able to access sensitive patient data, a violation of HIPAA, GDPR, and patient trust. Restricting access and blocking unauthorized communications protects both your organization and your patients.

---

[7] "OCR Lifts HIPPA Penalties for use of COVID-19 Vaccine Scheduling Apps," HealthITSecurity.com, Jessica Davis, 20 January, 2021
[8] "Threat Detections on Healthcare Endpoints Jump 60% in 2019," HealthITSecurity, Jessica Davis, November 13th, 2019
[9] Hospital Devices Left Vulnerable, Leave Patients at Risk," CSO, Ryan Francis, February 9th, 2017

Conclusion

IoMT devices are becoming indispensable in optimizing healthcare outcomes, but security is a growing concern. We must find ways of applying robust management and user protections. As the CISO of Boston Medical Center hospital puts it "We can't prohibit availability for the sake of security. We have to find a balance..."[10]

To secure IoMT systems, hospitals, and healthcare groups are moving towards comprehensive security architectures with rapid discovery engines, high visibility, customizable policy management tools, and strict enforcement. Implementing a unified security system with integrated components to protect your unique architecture will help protect you from emerging threats.

Invest in the tools to improve your IoMT security posture. Put everyone on track towards achieving better health. For more information about securing healthcare systems, read our healthcare security whitepaper, or reach out to your local Check Point representative.

---

[10] "How Healthcare Organizations Handle Endpoint Management," HealthTech, Tommy Peterson, October 21st, 2019

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com