50 Years of Growth, Innovation and Leadership

Medical Device and Network Security

Coming to terms with the Internet of Medical Things (IoMT)

A Frost & Sullivan White Paper
Sara Mitran

FROST & SULLIVAN

CONTENTS

INTRODUCTION

According to Frost & Sullivan's Internet of Medical Things (IoMT) Forecast to 2021[1] report, by 2020, 20 billion to 30 billion connected IoT and medical devices are expected to be a part of the healthcare ecosystem. This explosion of connected devices in the already vulnerable healthcare sector is a growing concern for healthcare providers, medical device manufacturers, the government, and the public at large. The emergence of IoMT as a part of everyday healthcare practice is alarming after failing to adopt basic security protections. Healthcare will increase its attack surface rather than shrink its attack surface.[2] Concerted efforts to address these issues have been largely focused on pre-market devices, but the realization of the existence and use of large fleets of legacy medical devices has resulted in new post-market guidelines and regulations, including recalls. Neither replacement nor re-certification of medical devices currently in use is an attractive option due to the cost and complexity involved. Innovative approaches to protect network security and prepare for the inevitability of the IoMT explosion are needed to ensure quality care delivery, consistent outcomes and the financial health of healthcare institutions.

1 Frost & Sullivan, Internet of Medical Things, Forecast to 2021, June 2017

2 Healthcare IT News, https://www.healthcareitnews.com/news/wannacry-petya-1-year-later-good-bad-and-ugly, June 29, 2018

IoMT SECURITY CHALLENGES

The FDA is regulating post-market medical devices because most devices currently used in hospitals were never meant to network outside a single hospital or even beyond an individual workstation. As a result, these medical devices do not contain embedded security capabilities. For instance, many older medical devices run unsupported operating systems (OSs)—such as Windows 95, 98, 2000—and can no longer be patched against vulnerabilities. Other common issues are hardcoded or default passwords that are not changed as well as a lack of anti-virus or personal firewall capabilities. Furthermore, some medical devices are controlled by clinical staff outside of the IT department's purview or the actual medical device manufacturer, while others require a physical connection to a specific workstation (which does not possess encryption capabilities).

Upgrades to these medical devices to enhance security would mean a costly and extremely time-consuming recertification process. Furthermore, the sheer volume of vulnerable medical devices makes them impractical and prohibitive to replace. Therefore, the likely response to working medical devices has been inaction, even though the security of these devices is a liability and a risk to clinical, operational and financial functions of every healthcare facility.

MEDICAL DEVICE ANALYSIS OF THREATS

According to the AHA's Fast Facts on US hospitals 2019 report, there are a total of 931,203 beds.[3] If an average hospital room has between 15-20 medical devices[4] that would mean that there are approximately 18.6 million medical devices in US hospitals. This number excludes any personal devices from clinical and non-clinical staff, such as tablets, laptops and smartphones, which are connected to the hospital's network, increasing the total number of devices within the hospital's IT network.

Medical devices include infusion pumps, insulin pumps, patient monitors, medical lasers, heart-lung machines, imaging systems (PET, CT, etc.), ventilators and extracorporeal membrane oxygenation machines, to name a few. Each room includes at least one infusion pump[5] and multiple monitors. Because infusion pumps and monitors are connected to a specific patient and have a direct impact on a patient's care, as compared to other medical devices, it is imperative that these types of medical devices are protected.

Insulin or infusion pumps are medical devices that pose a higher security risk. Not only are these pumps connected to a specific patient for the entire hospital stay, but insulin and infusion pumps can also be hijacked[6] to deliver a different dose than prescribed (either lower, higher or no dose at all). This could potentially lead to patient death or injury.

3 AHA, Fast Facts on US Hospitals, 2019, January 2019, www.aha.org/statistics/fast-facts-us-hospitals

4 HIT Infrastructure News, IoT Sensors Critical to Successful Health IT Infrastructure, Elizabeth O'Dowd, March 2, 2017, https://hitinfrastructure.com/news/iot-sensors-critical-to-successful-health-it-infrastructure

5 Healthcare IT News Security, Cybersecurity for Networked Medical Devices Pose Huge Risks to Patient Safety, Mike Miliard, February 29, 2016, https://www.healthcareitnews.com/news/cybersecurity-pro-networked-medical-devices-pose-huge-risks-patient-safety

6 Frost & Sullivan, Cybersecurity Threats and Medical Device Connectivity, 2016, www.frost.com

Average of 6.2 vulnerabilities per medical device

Product recalls from known security issues

60% of all medical devices are unpatchable (6 million-11 million)

Cyber-attacks directed at healthcare facilities were observed as of April 2018

Patient monitors may be accessed through an authentication bypass attack and can be instructed to issue a false alarm, disable alarms or display incorrect patient vitals.[7] Incorrect health information could lead to an erroneous assessment of the patient's medical condition, resulting in potential death or injury. Pump and patient monitor vulnerability can directly impact patient safety, a hospital's reputation and liability.

While imaging systems are not assigned to a specific patient, they handle patient data.[8] Imaging systems consist of any medical image capture, storage, or distribution equipment; any tool ranging from X-rays to digital imaging and communication (DICOM) workstations; and picture archiving and communication servers (PACS). Imaging patient data is transferred to different departments within a hospital and is transmitted to referring physicians frequently located outside of the inpatient setting. Medical devices and applications connected to outside elements pose a greater risk than applications solely connected inside. Imaging data could be compromised and/or altered, impacting a patient's health history or resulting in erroneous health-related decisions.

Challenged by design, medical imaging manufacturers have relied on the highly vulnerable Windows OS. Most imaging systems use the Microsoft Windows Embedded Standard Edition.[9] Imaging vendors supply patches for this specific OS; however, the patch has to be implemented at the hospital or health system to be useful.

In a recent KLAS research report, CIO and CISO respondents reported that about 33% of all managed connected medical devices at their facilities are "unpatchable."[10] Unpatchable medical devices are those that are no longer supported by their manufacturers because they were phased out, i.e., no longer in production or a newer version is available in the market. These unpatchable medical devices represent a large capital investment for hospital facilities. The disconnect between the hospital's expected product lifecycle and the manufacturer's expected product life is disconcerting. Until this disconnect is resolved, hospitals are still required to protect these unpatchable medical devices. Both patchable and unpatchable medical devices are vulnerable to attacks.

7 Ibid.

8 Ibid.

9 Tech Nation, Tech Tips: Which Operation System for Which Medical Device, Why and How to Patch It?, October, 1, 2017, https://1technation.com/tech-tips-which-operating-system-for-which-medical-device-why-and-how-to-patch-it/

10 Healthcare Innovation, CISOs, CIOs not confident in device security strategy, new research finds, Heather Landi, September 10, 2018, https://www.hcinnovationgroup.com/cybersecurity/article/13030781/cisos-cios-not-confident-in-their-medical-device-security-strategy-new-klas-research-finds

According to the newly formed Open Source Cybersecurity Intelligence Network and Resource (OSCINR), there is an average of 6.2 vulnerabilities per medical device, and the FDA has recently issued recalls for pacemakers and insulin pumps with known security issues. Founded by the FDA, Sensato-ISAO and H-ISAC, the OSCINR indicated that approximately 60% of medical devices are at the end-of-life stage with no security patches or upgrades available. Whether the total amount of end-of-life products is 33% as reported by the KLAS research or the 60% estimated by the OSCINR, it is still a baffling amount ranging between 6.1 million and 11.1 million devices. More importantly, medical devices were specifically targeted by cyber attackers as recently as April 2018.[11] If previous cyber-attacks have not been directed at healthcare and have been so disruptive to healthcare facilities, the impact of a cyber-attack targeting a healthcare facility could be disastrous.

WANNACRY

The May 12, 2017, Wannacry ransomware demanded bitcoin as ransom from those affected in exchange for the un-encryption of their own computer files. Wannacry infected over 300,000 computers across 150 countries (see Figure 2) and crippled hundreds of businesses in less than 24 hours, costing hundreds of thousands of dollars. The Wannacry cryptoworm targeted Windows OS computers without current security updates (i.e., unpatched) or those running unsupported versions of Microsoft Windows, such as Windows XP (when executed manually), Windows 7, and Windows Server 2003. A total of three Wannacry variants emerged. Five days later, new infections were slowed down with multiple counter attack measures implemented by security experts at large.[12]

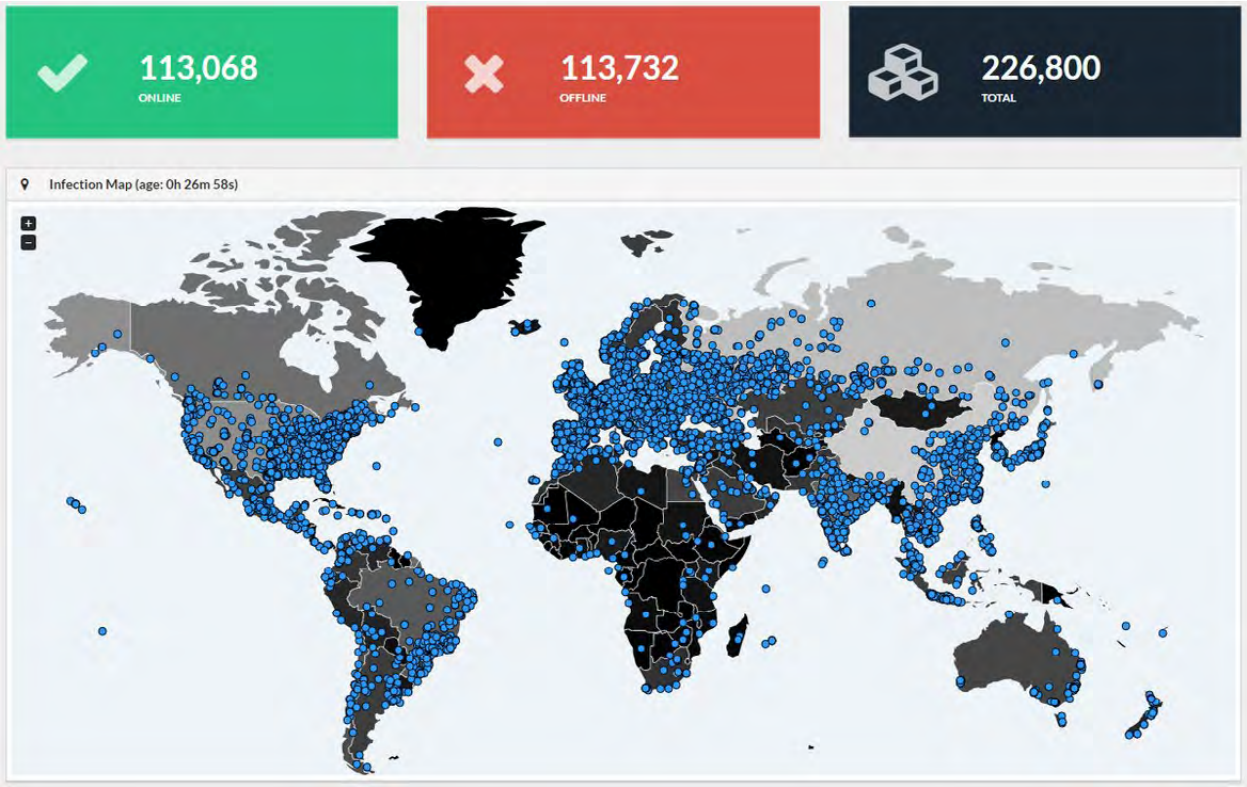
Even though the attack was not directed at healthcare facilities, the industry's consistent failure to support its IT systems with the most current security updates and common cybersecurity best practices made it particularly vulnerable. One system affected was the UK National Health Service (NHS). In fact, several NHS hospitals were paralyzed by their inability to identify impacted devices. Consequently, these NHS hospitals were unable to provide care to their patients.

One month later, the Petya wiper malware, which permanently damages victims' IT systems, impacted two US health systems among many other victims.

11 AEHIS, News, FDA Partners with Sensato-ISAO and H-ISAC to create Open Source Cybersecurity Intelligent Network and Resource, https://aehis.org/fda-partners-with-sensato-isao-and-h-isac-to-create-open-source-cybersecurity-intelligence-network-and-resource/

12 Malwareless, https://malwareless.com/wannacry-ransomware-massively-attacks-computer-systems-world/, May 12, 2017

FIGURE 1



Source: Wannacry World Attack Map

SETTLEMENTS, NEW REGULATIONS, AND RECALLS

Due to patient safety and privacy concerns caused by medical device security vulnerabilities, government officials have taken notice of pre-market devices. Settlement action is a punitive way to address post-market medical device mismanagement.[13] However, in recent years, Congress has established oversight committees and held hearings to identify risks and consider additional legislative actions to address the growing problem.[14] Since 2016, the FDA has developed policies and has issued recommendations to assist medical device manufacturers (MDMs) in managing cybersecurity regulations. This includes the Postmarket Management of Cybersecurity in Medical Devices[15] (Postmarket Cybersecurity Guidance) and the 2018 Medical Device Safety Action Plan.[16] The Action Plan stipulates the need for mandatory recalls when appropriate.

13 Healthcare IT News, https://www.healthcareitnews.com/news/md-anderson-pay-43-million-settlement-ocr-hipaa-violations, June 19, 2018

14 Medical Device Cybersecurity Report: Advancing Coordinated Vulnerability Disclosure. Medical Device Innovation Consortium. http://mdic.org/wp-content/uploads/2018/10/MDIC-CybersecurityReport.pdf, October 2018

15 FDA, Postmarket Management of Cybersecurity in Medical Devices, https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf, December 2016

16 FDA, 2018 Medical Device Safety Action Plan, https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM604690.pdf, April 2018

FROST & SULLIVAN'S PERSPECTIVE

Past efforts to protect healthcare security networks focused on email viruses and website phishing attacks. Growing pressure from the current post-market regulatory environment, recalls, and large settlements imposed for HIPAA violations present greater risks than ever before. These risks require mitigation with a programmatic security network approach. Healthcare systems have no option but to implement innovative network security to reduce risk from cybersecurity vulnerabilities. To mitigate today's cybersecurity threats, Frost & Sullivan recommends the following actions:

- Complete a thorough and comprehensive risk assessment to identify all devices and vulnerabilities
- Control IoMT communication down to "who" and "how"
- Enforce policies with full L2-7 visibility
- Initiate micro-segmentation
- Establish manageable and realistic network security parameters
- Maintain existing network assets and infrastructure

KEY POINT

Inaction is not an option

DEFENDER FOR IoT

The Extreme Networks Defender for IoT was designed exclusively for vulnerable IoT devices in the healthcare market. This is exactly what the IoMT environment requires. Defender uses whitelist policies to restrict who each device can communicate with and what each device can communicate, and then monitors all traffic to and from the device (with full Layer 2-7 visibility) to ensure that the device is operating according to its set profile. In addition, Defender segments IoMT devices into safe encrypted zones that extend from the devices to the data center to isolate and protect devices and their information from the rest of the corporate network.

Defender is designed to be simple to deploy and manage, and its user interface allows technical and clinical staff to onboard and move medical and other IoT devices easily and securely without IT staff intervention. Authorized users can also access operational information on each IoMT device, including location. This prevents clinical staff from needing to search for devices. Most importantly, Defender can be deployed on any network infrastructure without the need for network upgrades or changes—a requirement of other vendors' offerings—enabling healthcare companies to quickly enhance their security without worrying about a full infrastructure upgrade.

Extreme Networks is a leader in the wired and wireless LAN Access Infrastructure market and serves many industries, including healthcare. Every healthcare institution should consider Extreme Networks as a potential partner to secure networks and manage IoMT devices.

FROST & SULLIVAN

NEXT STEPS >

- **Schedule a meeting with our global team** to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.
- Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.
- Visit our **Digital Transformation** web page.
- Attend one of our **Growth Innovation & Leadership (GIL)** events to unearth hidden growth opportunities.

SILICON VALLEY | 3211 Scott Blvd, Santa Clara, CA 95054
Tel +1 650.475.4500 | Fax +1 650.475.1571

SAN ANTONIO | 7550 West Interstate 10, Suite 400, San Antonio, Texas 78229-5616
Tel +1 210.348.1000 | Fax +1 210.348.1003

LONDON | Floor 3 - Building 5, Chiswick Business Park, 566 Chiswick High Road, London W4 5YF
TEL +44 (0)20 8996 8500 | FAX +44 (0)20 8994 1389