An IDC InfoBrief, Sponsored by Fortinet | March 2020

Securing Medical Devices:

The Next Threat Vector

Research by Lynne A. Dunbrack, Group Vice President, IDC Health Insights

Executive Summary

Healthcare organizations face increasing security challenges as threat vectors evolve and increase in number and scope of attack. One such threat vector is medical devices connected to the healthcare organization's network. Medical devices are particularly vulnerable because of poor security practices and the sheer number of devices to secure across the enterprise. A typical 500-bed hospital could have between 5,000 and 7,500 connected medical devices at the bedside. Exploiting these vulnerabilities, cybercriminals can gain access to the network to exfiltrate valuable data assets, deliver ransomware, or severely compromise IT operations. Collateral damage to patient care is also a possibility when medical devices stop functioning correctly. While firewalls are part of the standard arsenal of security tools, they are not enough to protect connected medical devices against cyberattacks.

KEY FINDINGS

- » Healthcare organizations are increasingly at risk for medjacking, a cyberattack that exploits vulnerable interconnected medical device endpoints to gain access to healthcare IT systems and infrastructure
- » Medical devices are vulnerable to cyber attack because of the wide variety of device types and number of devices combined with poor security practices
- » Modest progress has been made in securing medical devices, despite more than half of IDC survey respondents reporting that they are piloting or have deployed intelligent medical device monitoring

Healthcare Organizations Face Increasing Security Challenges

Threat vectors are evolving, increasing in number and scope of attack

Today's healthcare organizations are at greater risk of a cyber attack than ever before given the proliferation of electronic health information, mobile and IoT technology, and connected medical devices. Hospitals are vulnerable to cyberattacks because clinicians and staff need around-the-clock access to mission-critical applications. Furthermore, cybercriminals are well aware that patch management is an ongoing challenge for understaffed healthcare IT organizations, especially as it relates to patching embedded systems in medical devices.

1.

Ransomware:

Preventing access to mission-critical IT resources

2.

Internet of Threats:

Expanding attack surfaces are increasingly borderless

3.

Vulnerable Endpoints:

Exploiting medical devices to launch an attack

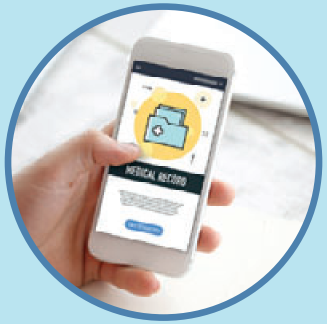
What is Medjacking?

Medjacking Defined: A type of cyber attack that exploits vulnerable interconnected medical device endpoints to gain access to healthcare IT systems and infrastructure.

Securing medical devices, which are increasingly connected to the network and interconnected with healthcare IT systems, is inherently complex. A device's embedded software is often not reliably patched and may no longer be supported (e.g., Microsoft XP). Cybercriminals can exploit these vulnerabilities to gain access to the healthcare organization's network. This type of attack is referred to as "medjacking."

A notable example is **MEDJACK.3**, a third version of a medjacking malware that is more advanced and poses a more serious threat than its predecessors. MEDJACK.3, a sophisticated zero-day attack, enables cybercriminals to steal patient data by targeting older operating systems that are prevalent in medical devices.

Why Are Medical Devices More Vulnerable than Other Internet-Connected Devices?



Medical devices represent a wide range of technology.

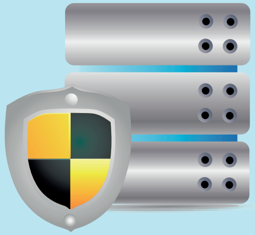
Devices include MRIs, CT scanners, bedside monitoring, ultrasound machines, and embedded devices such as pacemakers and insulin pumps. Many of these devices are run from mobile applications which need to be secured along with the mobile devices.

Manufacturers were reluctant to update systems software.

Medical device manufacturers believed that updating security software would require a new FDA 510(k) clearance approval. Also, they did not anticipate that their devices would be used as a target vector to attack IT systems.

Security practices have been poor.

Medical devices are more vulnerable to cyberattack due to a lack of system hardening, out-of-date patch levels, embedded operating systems that are no longer supported, and hardcoded or default passwords.



What is the Scale of the Challenge?

Securing medical devices is inherently complex because of the scale at which medical devices are deployed in a hospital setting.

10–15
connected medical devices per bed

×

925,000
total staffed U.S. hospitals beds

=

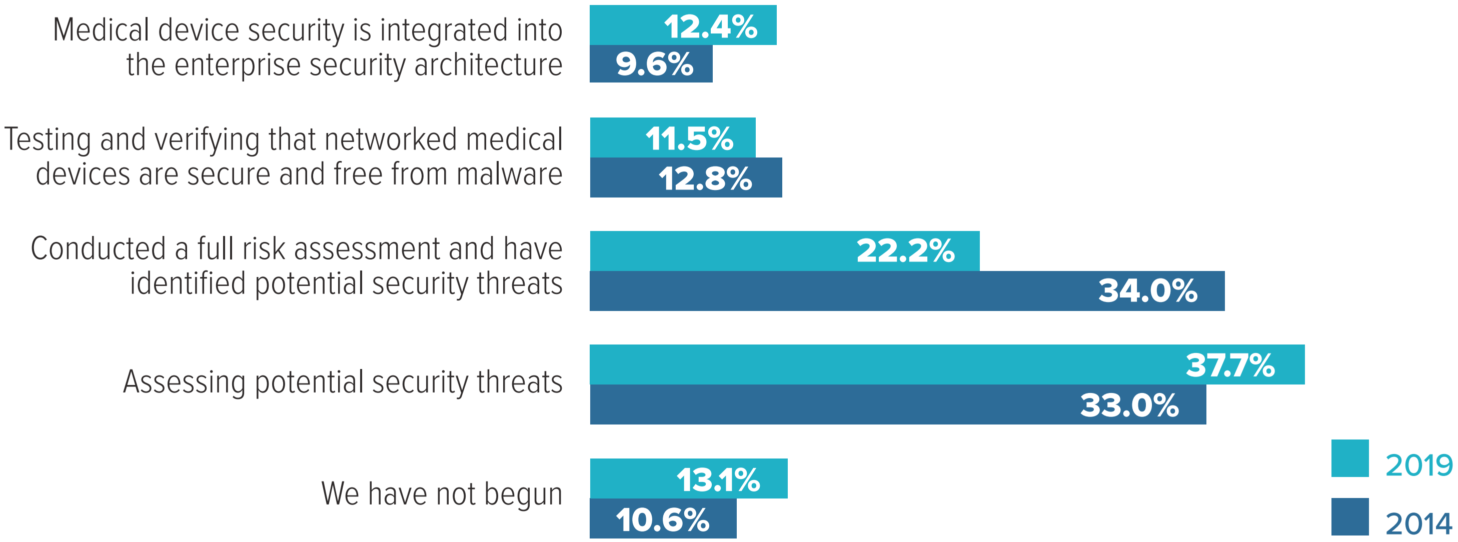
9.25–13.9
million
total bedside medical device devices

Source: https://www.aha.org/statistics/fast-facts-us-hospitals

Progress on Securing Medical Devices has been Modest

Despite **51.2%** of provider respondents reporting that they are piloting or have deployed intelligent medical device monitoring, modest progress has been made in securing medical devices over the past five years.

Q. *Which one of the following statements best describes your approach to securing networked (wired or wireless) intelligent medical devices?*



Source: IDC Insights Cross Industry Cyber Threat Survey, May 2014, n=94

Source: IDC, Global IoT Decision Maker Survey 2019, June 2019, n=333

Technologies Healthcare Providers Should Have in Place to Secure Internet-Connected Medical Devices

While firewalls are part of the standard arsenal of security tools, they are not enough to protect connected medical devices against cyberattacks.

4 Key Security Technologies for Securing Medical Devices

1. Network access control systems

2. Strong Authentication for IoT Devices

3. Internal segmentation firewalls

4. Software-defined wide area networking (SD-WAN)

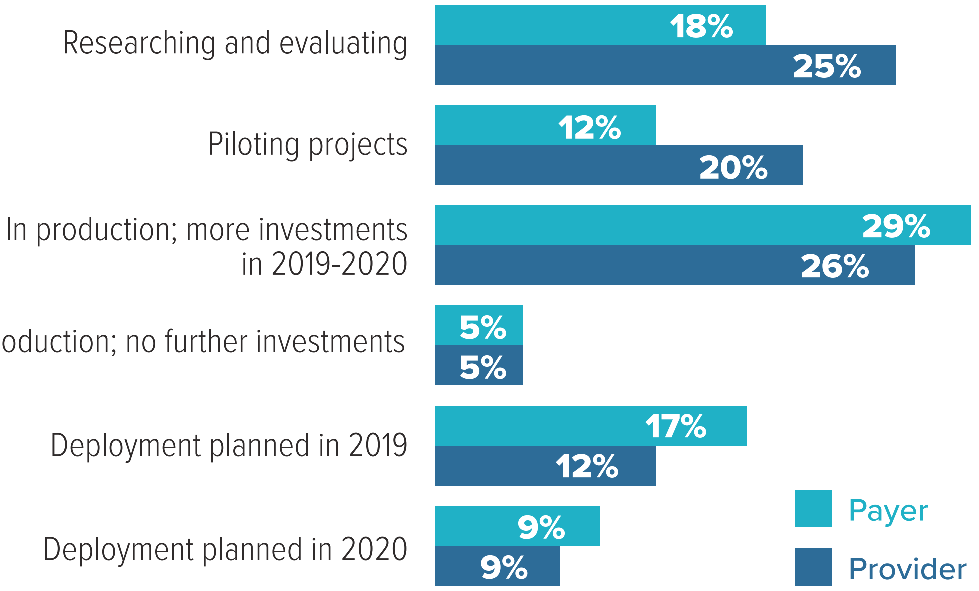
Implications for Consumer Medical Devices

Changes in reimbursement models are driving healthcare organizations to make steady progress in their investment in and deployment of connected remote health monitoring solutions.

The deployment of consumer medical devices should be included in security risk assessments. Increasingly clinicians are using patient-generated data to care for their patients; 60% of providers and payers indicated using patient generated data collected in real time, or near real time, for clinical interventions from alerts generated by FDA-cleared remote health monitoring devices.

Uploading patient data from consumer-grade medical devices to be stored in electronic health records creates its own security risk. Most consumer medical devices have companion mobile applications that can easily be compromised by malware. This combination of medical devices and mobile applications updating clinical systems serve to further exacerbate the borderless attack surfaces found in today's connected heath system.

Q. *What is the current state of your technology stategy to secure remote health monitoring?*



Payer N = 100, Provider N = 100

Source: IDC, Connected Health and Value-based IT Investment Plans Survey, February 2019

IDC CASE STUDY

Solution Snapshot

Organization: Heartland Dental

Operational challenge: Provisioning security at scale across an expanding enterprise nationwide

Solution: FortiGate, FortiManager, FortiAP, FortiExtender and FortiCloud

Benefits: Security at scale, automation, comprehensive training conducted by Fortinet

Best practices: Automate as much as possible to simplify network management; leverage training to ensure new and experienced staff keep up to date on evolving security technology and practices

Heartland Dental Delivers Security at Scale with Fortinet Solutions

“Heartland is able to offer dental practices a greater level of security than they ever expected.”

— Ross Petty, Senior IT Security Manager, Heartland Dental

Heartland Dental is a dental support organization (DSO) that provides non-clinical services such as marketing, human resources, and IT services including offsite backup, networking, and security to dental practices. Heartland Dental has grown rapidly over the years. At the end of 2019, it opened its 1,000th office and expects to add another 100 plus dental offices in 2020.

Given Heartland’s growth strategy, the ability to easily provision and manage technology at hundreds of remote dental practices was a key selection factor. After a comprehensive search, Heartland selected Fortinet over its competitors, including the incumbent vendor, because Fortinet’s offering is a “total package that provided an all-in-one solution that was cost effective,” stated Ross Petty, Senior IT Security Manager. FortiManager was a key component of that decision because it enables Heartland IT staff to provide centralized network management from a single pane of glass. With more than 1,000 practices in 37 states, security at scale through automation, total cost of ownership, and flexible solutions adaptive to new innovations are critical to Heartland’s long-term success.

Dentistry has evolved over the past decade with more dentists using connected medical devices and three-dimensional (3D) printing to offer innovative dental services to their patients. One such service is Invisalign teeth straightening that replaces uncomfortable and unattractive metal braces. Using the Itero wireless digital scanner, dentists can generate a precise 3D scan of the patient’s teeth to create a custom Invisalign treatment plan. As these services became more popular, more robust wireless connectivity was needed in Heartland’s remote offices. Heartland is deploying Fortinet’s cloud-based wireless access points and using FortiCloud to manage them. To provide an additional layer of security for connected medical devices, wireless networks are segmented using Fortinet’s internal segmentation firewall (ISFW).

The dental industry is adopting more modern technology as the demand for mobile apps, online appointments, and digital technology like 3D scanners continues to grow. Consequently, dental practices are becoming more vulnerable to security threats and will need to improve their security posture by deploying flexible security solutions that respond to rapidly evolving business, clinical, and technical requirements.

Essential Guidance

Develop an overarching security plan that includes all devices and device types in the cyberthreat assessment

Segregate medical devices and other valuable IT resources according to their risk posture

Increase visibility of medical devices at the edge and on the network

Deploy a platform solution / fabric that can automate enforcement

Form a strategic relationship with your security technology supplier

A MESSAGE FROM OUR SPONSOR

About Fortinet: Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. Worldwide, more than 425,000 customers trust Fortinet to protect their businesses.

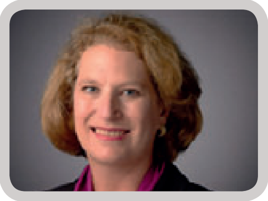
FORTINET®

Learn more about Fortinet Healthcare Solutions at
https://www.fortinet.com/healthcare

Contact healthcare@fortinet.com for a Cyber Security Threat Assessment.

Follow us @FortinetHealth on Twitter

IDC Analyst Profile



Lynne A. Dunbrack

Group Vice President, IDC Health Insights

Lynne Dunbrack is Group Vice President for Public Sector, which includes IDC Government Insights and IDC Health Insights. She manages a group of analysts who provide research-based advisory and consulting services for payers, providers, value-based health organizations, life science organizations, IT service providers, and the IT suppliers that serve those markets. Lynne also leads the IDC Health Insights' Connected Health IT Strategies program. Specific areas of Lynne's in-depth coverage include mobile, constituency engagement, interoperability, digital transformation, privacy, and security. Technology coverage areas include clinical mobility (physician facing) and mobile health (consumer facing), end-to-end remote patient health monitoring for health, wellness and chronic conditions, Internet of Things (IoT), telemedicine and virtual care, and digital therapeutics.

IDC Corporate USA

5 Speen Street
Framingham, MA 01701
USA
T: 508.872.8200
F: 508.935.4015
Twitter: @IDC
idc-insights-community.com
www.idc.com

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship in noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.