



5 BEST PRACTICES FOR MITIGATING MEDICAL DEVICE SECURITY RISKS

Most healthcare institutions have made significant security investments over the past three years in order to protect patient and organizational data from breach. However, most hospitals are still trying to navigate the increased attack surface caused by connected medical devices. Experts have identified at least fifteen IoT attack surfaces¹, each with their own list of potential vulnerabilities.

Concern over code modification, key compromise, password-based vulnerabilities and man-in-the-middle attacks have caused hospital CIOs and CISOs to rethink their security strategies and investments. The threat to these devices has even been assigned its own term: medjacking, a shortened form of “medical device hijacking.”

Healthcare organizations have significantly more to consider than the average business when it comes to network and device security. For a hospital, an attack on medical devices means risk to patient care and safety. The outcome of these attacks can put lives, patient trust and the growth of the healthcare organization at risk. This paper outlines five best practices to mitigate these risks.

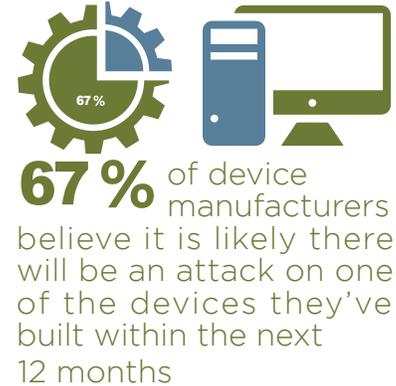
1. REQUIRE A SECURITY REVIEW DURING THE PROCUREMENT PROCESS

It's no secret medical devices should have stronger inherent security than they have today. Many do not have appropriate password complexity, data encryption or modern operating systems in place. Because of this, 67% of device manufacturers believe it is likely there will be an attack on one of the devices they've built within the next 12 months.²

To assist in this area, the U.S. Food and Drug Administration (FDA) has begun to publish pre-market and post-market guidance on managing device security risks. However, there are not yet many binding requirements for medical device security.

Healthcare organizations should require a security review take place before the procurement process is complete and should ask questions such as:

- What type of data will the medical device create, store and transmit?
- Does the medical device encrypt data in-transit and at rest?
- Does the medical device allow the password to be changed by the administrator, and does it support appropriate password complexity?
- What operating system is used?
- How will patch management of the device take place?
- Does the device contain USB or other removable media ports?



More than **70%** of network segmentation projects in **2017** would need to be **re-architected**



2. REVISIT YOUR NETWORK SEGMENTATION STRATEGY

Network segmentation is core to a healthcare system's network security strategy, and yet, it is difficult to do well. Organizations fall into the trap of either over-segmenting or under-segmenting their networks. In fact, analysts expected more than 70% of network segmentation projects in 2017 would need to be re-architected because of over-segmentation³. So why is it so hard to find the right level of network segmentation for a given

organization? One reason is that organizations lack an understanding of what types of endpoints are connecting to the network—and what data they are accessing.

Experts recommend healthcare institutions segment based on data sensitivity, location and criticality, and place less emphasis on things such as organizational structure. For example, hospital departments should be grouped within a single zone, and new zones should only be created for endpoints that access more sensitive data. Another recommendation is to group like resources together.

2. Ponemon Institute May 2017, <https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/medical-device-security-ponemon-synopsys.pdf>

3. Gartner Research 2016, Best Practices in Network Segmentation for Security

4. Gartner Research 2016, Best Practices in Network Segmentation for Security

For example, Internet of Things (IoT) and medical device technology should be zoned together, with a separate zone for those endpoints that access HIPAA information. Organizations should ask themselves “Is there a strong security case to keep these resources apart?”⁴ Network visibility, discussed in the next section, can provide the endpoint information needed to make these decisions.

3. IDENTIFY AND INVENTORY ALL MEDICAL DEVICES



Creating an inventory of all endpoints attached to the network is the first step a CIO should take to effectively manage IoT risks

Network visibility is the first step to mitigating the risk of connected medical devices. In order to secure a device, you must first know it exists. Gartner lists creating an inventory of all

endpoints attached to the network as the first step a CIO should take to effectively manage IoT risks.⁵ Gartner recommends this be done automatically, if possible, or performed manually no less than twice a year.

In order to reduce the burden of identifying all medical devices on the network, organizations are implementing IoT security profiling systems to find devices automatically. The goal of these systems is to generate an up-to-date and comprehensive equipment inventory that can be used to identify information such as how many devices are on the network, what types of devices they are and where they are located. This data can be used to verify the accuracy of device management contracts, reduce the risk of over-purchasing equipment as well as develop a more holistic network security strategy.

The concept of endpoint profiling utilizes something almost every device has: a Media Access Control (MAC) address. MAC addresses are unique to the device and can help to identify the device manufacturer. Other information used to identify and profile the device can be found through a variety of collection sources, including DHCP, SNMP polls/traps, NetFlow/J-Flow, Active Directory and RADIUS Accounting.

4. ONBOARD MEDICAL DEVICES SECURELY

Onboarding medical devices is more difficult than it is for traditional endpoints since most cannot hold the supplicant required for traditional 802.1X authentication systems and must rely on MAC Authentication Bypass (MAB). This means that when a port is unable to authenticate a newly-connected device using 802.1X, it will attempt to authenticate the device using its MAC address as the equivalent of a username/password credential.

If the MAC address is included in a directory or device database, the device is granted a pre-determined level of network access, which might initially be a restrictive network segment. Once the device's profile is fully and accurately determined (e.g. the device is determined to be an approved model of an infusion pump), it can automatically be moved to its designated network segment. All devices that are not pre-approved are either blocked from gaining any access or are placed in “quarantine” in an isolated VLAN, depending on the institution's policy.

An endpoint profiling system can enable administrators to assign network access privileges with full knowledge of what each device is and, therefore, what its legitimate functions should be during onboarding. The result is a much more granular and secure method of using MAC authentication to enforce access privileges or restrictions.

5. Gartner Research 2017, Best Practices for Healthcare Provider CIOs to Effectively Manage IoT in the Hospital

5. MONITOR ALL MEDICAL DEVICE BEHAVIOR

Research has shown the mean time to identify a breach



is six months (190.7 days)

Continuous monitoring of medical device behavior is a critical component to identifying threats in real time—something we know is desperately needed since research has shown the mean time to identify a breach is six months (190.7 days).⁶ Imagine how much damage can be done in that six-month timeframe. And, imagine having to explain to regulators or opposing counsel during discovery in a civil lawsuit why the breach was not found and contained earlier. If an endpoint profiling system is in place, it is actively profiling endpoints

to not only identify the type of device, but also how it should behave on the network. The system can then continuously monitor network communications to detect any unusual or high-risk activity that would require security investigation.

Profiles can be made so that unusual attempts to access resources that might contain ePHI are relatively easy to detect. For example, a medical device with a proprietary operating system suddenly identifying as a general-purpose PC would indicate a potentially threatening change in its identity. Even more threatening would be the anomalous behavior of a medical device attempting to upload files via an outbound FTP session.

Healthcare organizations should look for systems that offer flexible enforcement actions to balance the unique availability and security requirements found within healthcare. This can include an automatic alert followed by manual investigation and intervention or automatic enforcement actions such as device-to-re-authentication, quarantining a device to an isolated VLAN or blocking its access entirely through shutting down a port.

THE PATH TO SAFE PATIENT CARE

Medical devices have had a profound impact on the quality of healthcare. Whether stationary, bedside or portable, these devices help improve patient outcomes, accelerate recovery times and minimize readmissions. But while creating better outcomes for patients, these systems are putting hospital and clinic networks at a substantially greater risk of attack. Medjacking has become a pervasive and serious threat. A breach of protected health information caused by medjacking can expose a healthcare institution to significant fines and costly litigation, not to mention put patient safety at risk.

IoT security systems that focus on device discovery and profiling are purpose-built to provide the visibility and control actions that healthcare organizations require. Working in concert with the existing network infrastructure, such systems identify all medical devices the instant they connect to the network, onboard them to the correct network segment according to security policy and continuously monitor their activity to detect uncharacteristic behavior. With these capabilities in place, hospitals and healthcare systems can confidently embrace the medical devices that help support their patients and their business.

6. <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SELO3130WWEN>