MEDIGATE

The Internet of Medical Things: Why Traditional IoT Security Isn't Enough

Connected Medical Devices are Easy Targets

Healthcare delivery relies heavily on connected medical devices. They enable tremendous increases in productivity, efficiency, and accuracy, but at the same time, they enlarge healthcare's attack surface. Adding hundreds or thousands of medical devices to a hospital network offers attackers more targets, and many of those devices were never designed with security in mind. Others are not patched or updated regularly. As a result, vulnerabilities that were remedied long ago by software providers in other industries can still be exploited through connected medical devices simply because they are difficult to patch or the risk of interfering with their functionality is deemed to be too high. They are low-hanging fruit for cyberattackers.

Cyberattack vectors also have diversified quickly. There are many ways - and reasons - for malicious actors to attack connected medical devices. The Association for the Advancement of Medical Instrumentation (AAMI) organization's Principles for Medical Device Security[1] report categorizes them into three main groups:

Target devices

Medical devices attacked directly to collect the information they contain or to interfere with their operation. Implantable medical devices (IMDs), such as cardiac implants, insulin pumps, and neurological implantable pulse generators (IPGs) usually contain personal information stored in their memories, which can be used by an attacker for social engineering and identity theft. Technical data can be used to facilitate attacks relying on specific health problems[2]. A wide range of IMDs has been shown to contain potentially lethal security flaws[3]. Connected medical devices also can be targeted and held hostage in ransomware attacks.

Pivot devices

Attackers use connected medical devices as footholds to establish network presence. Once in, advanced attackers conduct reconnaissance, looking for pathways to valuable assets in the healthcare network, such as Patients Health Information (PHI). The hacker group, Orangeworm, has successfully infected medical imaging systems in the United States and appears to be targeting sensitive data, protected health information, and intellectual property.

"Drive-by" attacks

In May 2017, WannaCry attacked unpatched Windows-based systems. Many connected medical devices running on Windows were infected, causing medical procedures to be cancelled and patients to be referred to alternative medical centers. Malware also can cause unintended malfunctions in medical devices.

1. AAMI TIR57:2016, Principles for medical device security – Risk management. Retrievable from: http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729

2. Security of implantable medical devices with wireless connections: The dangers of cyber-attacks, Taylor & Francis Online, June 13, 2018 https://www.tandfonline.com/doi/full/10.1080/17434440.2018.1483235

3. Pycroft L, Boccard SG, Owen SLF, et al. Brainjacking: implant security issues in invasive neuromodulation. World Neurosurg. 2016; 92:454–462

Trying to Protect the Invisible

Unlike connected devices in traditional Internet of Things (IoT) deployments, attacks on devices in the Internet of Medical Things (IoMT) can have fatal consequences for patients, as well as devastating implications for healthcare providers' reputations. Protecting connected medical devices poses several unique challenges that traditional IoT security solutions cannot address.

Medical devices are often closed systems, running legacy software, or deployed behind secondary firewalls managed by the device manufacturer. In these cases, security professionals and traditional security products cannot access them[4]. One hospital experienced malware infections in three blood-gas analyzers - in spite of having a firewall, heuristics-based intrusion detection, endpoint security, antivirus tools, and an experienced security team. Each system had a backdoor with access to the hospital's internal network. By the time the malware was discovered, hospital data records had been exfiltrated to Europe.

Security solutions designed for traditional IoT environments try to identify every device on the network and classify it based on its business function.

> **They learn communication behaviors and create conversation maps but they have little to no clinical context or understanding of what is critical in a healthcare setting.**

These security solutions simply treat medical devices the same way they treat every other business device. With a traditional IoT security solution, the hospital's IT and BioMed teams may be able to identify some of the medical devices connected to the network, where they are on the network, and if they are sending packets. However, traditional IoT security products cannot identify each device with the granularity needed to protect it - The IT team can't protect what it can't see and accurately assess risk without detailed visibility.

Trying to Detect the Anomalous

Securing enterprise networks is a complex proposition on its own. Adding medical devices to a network takes complexity to a whole new level. Securing medical devices requires detailed knowledge of each and every medical device and a comprehensive understanding of medical workflows. Dozens of different device types, thousands of devices from different manufacturers, and a mix of protocols and operational parameters make it nearly impossible for a typical IoT security solution to accurately detect anomalies and provide the insight needed by the IT and security teams to respond appropriately.

> **Traditional IoT security solutions can't fingerprint medical devices with the specificity needed to understand their manufacturers' communication protocols.**

As a result, they can only detect superficial suspicious network behaviors—activity that would be flagged in a corporate IT network regardless of device type. For example, a traditional IoT security solution will see packets being transferred between two network nodes, but without the necessary medical context, it will not comprehend that the nodes represent a fetal monitor communicating with an IV pump, which is out of scope from the manufacturer's protocol and might indicate a threat.

Because IoT solutions generate basic security alerts and lack clinical domain expertise, they cannot prioritize risks or contribute to providers' risk management plans.

And without prioritized alerts and device-specific risk assessments, precious time could be spent on low-level risks and devices while high-level risks go unnoticed.

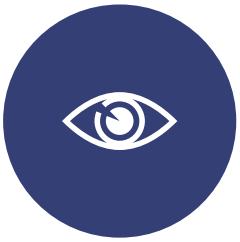
Trying to Prevent the Inevitable

If network and traditional IoT security solutions were enough, medical devices would already be secure. Healthcare providers are aware of the risks associated with connected medical devices. A study from June 2018 conducted by HIMSS found that 85% of surveyed healthcare providers consider medical device security a strategic priority[5]. But until now, security solutions for connected medical devices have lacked the specific capabilities needed to make them successful.

4. When medical devices get hacked, hospitals often don't know it, Healthcare IT News, May 11, 2018 https://www.healthcareitnews.com/news/when-medical-devices-get-hacked-hospitals-often-dont-know-it
5. http://outreach.unisys.com/MedicalDeviceManagementPulseSurveyResults

The First IoMT-Specific Security Solution

As the first platform dedicated to securing medical devices, Medigate protects all of the connected medical devices on healthcare providers' networks. The Medigate platform fuses the knowledge and understanding of medical workflows with device identities, protocols, and networking expertise to provide complete visibility into devices and risk, detect behavioral anomalies, and actively block malicious activities. Medigate enables providers to ensure critical treatment delivery and protect patient privacy.



Gain Detailed Visibility

The Medigate platform is the only solution that has cataloged thousands of medical devices, enabling it to discover and precisely identify all connected medical devices on a provider's clinical network. Medigate fingerprints all devices using deep packet inspection (DPI) techniques, allowing dynamic medical device inventory management. Data gathered from DPI is used to calculate a device's risk score, which can be correlated with medical device standards and clinical parameters to inform risk assessment. Now the IT team knows exactly what is connected, where it's located, and the security posture associated with each and the BioMed team knows how many devices they have, where they are and what software versions they're running, among other things.

Detect Threats in Real Time

Only Medigate has the contextual understanding to accurately detect credible threats. The platform understands medical device protocols, existing and potential cyber threats, and expected device behavior. It meticulously analyses device and network communication, as well as medical workflow patterns, to accurately detect anomalous behavior and identify threats in real time with minimal false positives.

Prevent Attacks from Succeeding

The Medigate platform blocks malicious communications in real time without affecting the operation of the medical device under attack. Intelligence gathered through the platform's visibility and detection capabilities is used to further build protection around connected medical devices. Medigate data can be integrated with traditional NAC and firewall solutions to improve policy deployment and enforcement. Granular policy enforcement allows more efficient VLAN and ACL assignment and enables remediation of threats detected by Medigate.

MEDIGATE

An IoMT Solution for Today's Healthcare Cyberthreats

Medical-grade devices require medical-grade device security.
For more information about the Medigate platform, visit **www.medigate.io**
or contact your local account representative at **info@medigate.io**