FORTINET

Securing Medical Device Manufacturers and the IoMT

Protecting Your Expanding Threat Surface

Table of Contents

Overview

In the ever-evolving landscape of healthcare, medical device manufacturers everywhere are dedicated to ensuring high-quality products, safety, and treatment machines. However, with the rapid growth and innovation of connected medical devices and the Internet of Things (IoT), the cybersecurity threat landscape has expanded within the industry, increasing the attack surface and vulnerable access points of your products.

In light of these increased risks, spending on cybersecurity in the medical device sector is forecast to grow from **$869 million** to **$1.2 billion** between 2020 and 2025, accounting for about **11.3% of health cybersecurity expenditure.**[1] This substantial investment reflects the industry's recognition of the growing threat landscape and the need to protect manufacturers from the damaging effects and liabilities of cyber intrusions.

The aftereffects of cyber intrusions for medical device manufacturers can be detrimental. Network vulnerabilities can compromise private data confidentiality and integrity, opening medical device manufacturers up to legal issues in the event of a cybersecurity breach. In addition, the loss of trust or goodwill may significantly impact profitability and business growth.

Recognizing the urgency of the situation, regulators have introduced measures such as the PATCH Act and the FDA's Ensuring Cybersecurity of Devices, placing pressure on manufacturers to act swiftly and implement comprehensive security measures for medical devices. While the PATCH Act now requires medical device manufacturers to follow security-by-design practices that harden their products against attack, it is crucial for manufacturers to go beyond these requirements and adopt additional precautions to secure their own networks and supply chain. A holistic approach ensures a comprehensive effort toward enhancing the cybersecurity of medical devices.

Fortinet's cybersecurity experts understand the specific risks, regulatory measures, and key technologies involved in securing the Internet of Medical Things (IoMT) for manufacturers to protect devices and maintain industry viability.

Risks Specific to Medical Device Manufacturers

Medical devices operate within a unique risk landscape, characterized by distinctive vulnerabilities that demand advanced, proactive attention. Standard, legacy operating systems that cannot be updated by the end customer are susceptible to mainstream attacks. The presence of insecure embedded, real-time operating systems and the complex challenge of extensive testing requirements necessitates proactive measures to mitigate potential threats to ensure the security and reliability of medical devices.

Standard operating systems:

Medical devices often run standard operating systems, such as Windows or Linux, which not only expose them to mainstream attacks but also pose a greater risk due to their inability to receive regular patches and updates like normal computing devices. For instance, the WannaCry ransomware attack in 2017 targeted outdated Windows systems in healthcare organizations, causing disruptions in patient care and emphasizing the vulnerability of medical devices to such attacks.[2]

Insecure embedded/real-time operating systems:

Not all embedded/RTOS are designed or manufactured with strong security measures, posing multiple undiscovered vulnerabilities. For example, an insecure RTOS might lack proper isolation mechanisms, allowing an attacker to compromise the device and potentially gain unauthorized access to sensitive data or manipulate critical device functions post-manufacturing.

Extensive testing requirements:

Rigorous safety and accuracy testing in manufactured medical devices result in longer remediation periods once vulnerabilities are identified. Patching vulnerabilities and implementing security measures in medical devices may involve complex and time-consuming processes, which can impact time-to-market and product availability. The challenge lies in striking a balance between meeting regulatory requirements, ensuring the security of the device, and maintaining efficient development timelines.

Why Medical Devices are Prime Targets for Cyber Attackers

Medical devices have become a central focus for cyber attackers due to several compelling factors which highlight an urgent need for robust security measures in medical devices to avoid devastating breaches.

- **Patient PII value in fraudulent activities:** Private information stored on manufacturers' medical devices has an immense value that threat actors can profit from by selling on the dark web.
- **Blurred lines of responsibility:** The division of security responsibilities between device manufacturers and their users can become unclear, leaving devices unsupervised and susceptible to attacks. Each of the medical devices currently on the market has on average 6.2 vulnerabilities to cyberattacks.[3]
- **Sheer number of devices:** Medical devices are typically used by large organizations, such as hospitals, which face the challenge of overseeing thousands of devices, making it difficult to ensure sturdy security measures for each one.
- **Increased security risks from diverse technology:** Utilizing a mix of older and newer technologies, alongside third-party components, introduces additional security risks due to older systems lacking necessary security features and third-party components undergoing inadequate scrutiny. Medical device hardware can have a lifespan of 10 to 30 years, but the underlying software life cycles, determined by manufacturers, can vary from a few months to the device's full life expectancy. This extended time frame allows threat actors ample opportunity to discover and exploit vulnerabilities.
- **Inability to upgrade legacy systems:** Medical devices often run on outdated and closed systems, making it difficult for end users to upgrade them. This situation creates security vulnerabilities that attackers can exploit due to limited updates and security mechanisms that depend solely on the manufacturer's support. While 32% of medication dispensing systems are functioning on unsupported versions of Windows, 19% of all devices are performing on unsupported operating systems.[4]

Emerging Trends Within the Medical Device Sector

Medical device manufacturers are adopting connected medical devices at a rapid pace. The IoMT market size has an expected growth rate of 23.4% CAGR by 2028[5], and medical device manufacturers must stay on top of how the market is leveraging their products, what potential threats are surfacing that put them at risk for cyber intrusions, and the importance of device security, all while demonstrating value-based care.

Here are trends to look out for:

The global use of medical devices is set to surpass over 50 billion within the upcoming decade[6] as the acceleration of new medical technology continues to advance. With the rise of virtual medical treatment and connected cloud apps of wireless and wearable technology, private data is actively being stored and sent across networks.

Ransomware threats are evolving and becoming more complex for attacks on medical devices. With former focus on ransomware groups like Daixin Team and Hive, a new cyber threat has emerged. Venus ransomware infiltrates remote desktop services running on Windows within medical centers to encrypt files and steal critical information on medical devices.

The surge of cyber risks for healthcare third parties such as device manufacturers are on the rise. These types of attacks arise when critical and private information is stolen from a third party or when their systems are compromised and utilized as a means to access and capture sensitive data stored on your systems, putting medical device manufacturers at risk of a data security breach.

Key Technologies for Medical Device Cybersecurity

In securing medical devices, specific technologies play a pivotal role in fortifying the defense against cyber threats. By effectively implementing these key cybersecurity guards, medical device manufacturers can enhance the security of their IoMT ecosystem and mitigate potential threats to device safety and data integrity.

- **Secure Boot:** Secure Boot ensures that only authenticated and trusted software components are allowed to run during device boot-up. It helps prevent unauthorized or malicious software from compromising the device's security.

- **Device encryption:** Implementing encryption mechanisms, such as strong cryptographic algorithms, helps protect sensitive data stored on the device. Encryption ensures that even if the device is compromised, the data remains unreadable and unusable to unauthorized individuals.

- **Secure firmware updates:** Manufacturers should utilize secure methods for updating device firmware to address vulnerabilities and introduce new security measures. Secure firmware update mechanisms, such as code signing and encryption, prevent unauthorized modifications and ensure the integrity of the update process.

- **Security event monitoring and response:** Many devices are not monitored for security events, and solutions exist to help manufacturers gain visibility into potential threats within the IoMT ecosystem. They collect and analyze security events and logs from various devices and systems to detect and respond to security incidents in real time. This provides manufacturers with insights into security threats, enabling them to proactively mitigate issues.

- **Penetration testing:** Conducting regular penetration testing helps identify vulnerabilities and weaknesses in the device's security. By simulating real-world attacks, manufacturers can discover and address potential security gaps before they are exploited by malicious actors.

Protecting the Medical Device Ecosystem

Ensuring the cybersecurity of medical devices is not just about securing individual devices; it requires a comprehensive approach that adds an additional layer of protection to your ecosystem. By adopting a layered defense for your cybersecurity strategy, medical device manufacturers can protect their devices, networks, critical data, and overall business operations.

Fortinet aims to ensure the wide-ranging protection of the medical devices you deliver, keeping the data, networks, and systems around them safe. We offer an integrated platform and a secure environment that enables manufacturers to implement proactive security measures throughout the medical device lifecycle. Fortinet's scalable and flexible solutions address the unique challenges faced by medical device manufacturers in today's threat landscape.

Our expansive suite of solutions includes security for network, application, cloud, and mobile environments. With features like secure remote connectivity, endpoint device security, and AI-driven threat protection, we provide the necessary safeguards for an extensive cybersecurity posture. These include:

FortiGate gives device manufacturers a protective layer that allows them to patch zero-day vulnerabilities in isolation without compromising the device. It also gives them a toolkit of network capabilities.

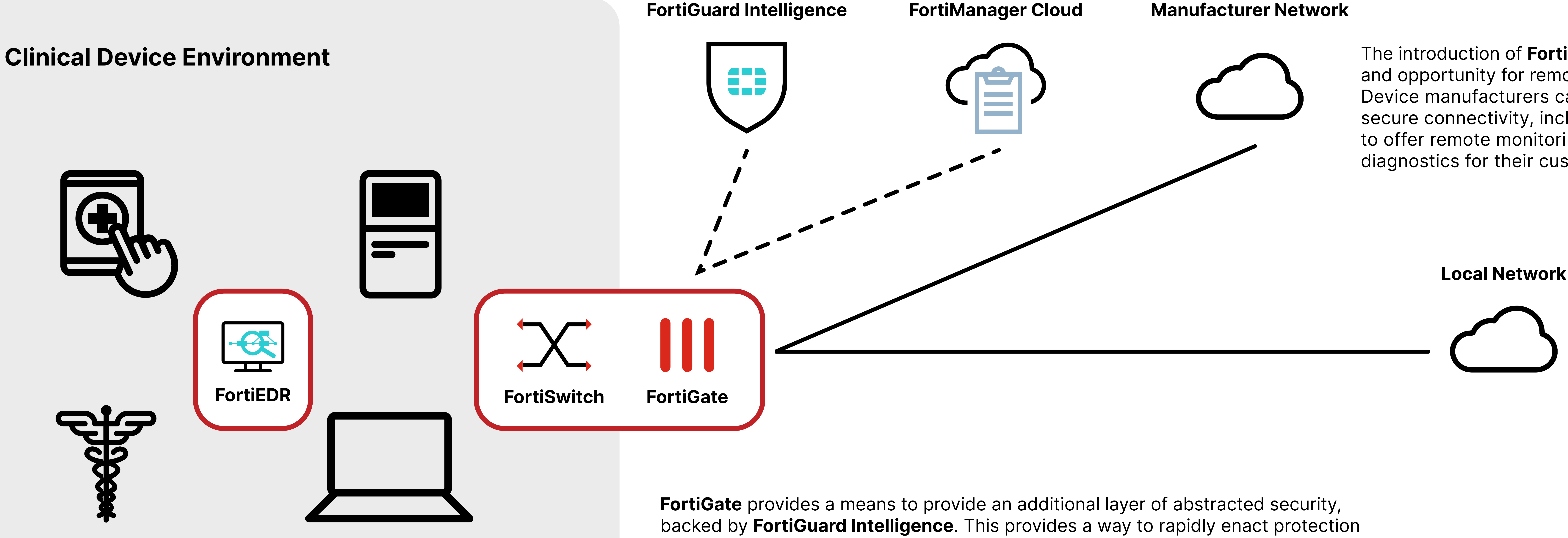
FortiSwitch provides micro-segmentation for multiple connected devices in a solution.

FortiEDR enable policies to be hardened so that only approved processes may run on the device OS.

FortiCloud Manager adds cloud-based management capabilities to FortiGate.

FortiGuard Intelligence gives FortiGate access to rapid AI-driven security and threat updates.

Clinical Device Environment



The introduction of **FortiGate** offers and opportunity for remote connectivity. Device manufacturers can leverage secure connectivity, including LTE/5G, to offer remote monitoring and diagnostics for their customers.

A clinical solution could be several interconnected devices in a contained environment or could be a single device.

FortiGate provides a means to provide an additional layer of abstracted security, backed by **FortiGuard Intelligence**. This provides a way to rapidly enact protection for new threats.

The introduction of **FortiSwitch** can enable microsegmentation between devices within the environment, where individual traffic policies can be extended down to the port level.

FortiEDR can be used to further harden Windows and Linux-based devices.

From Protection to Progress: Advancing Medical Device Security

It is important for medical device manufacturers to work closely with a partner that offers them a practicable approach to augmenting their security. Fortinet's consistent, end-to-end risk mitigation and total assurance frees your teams up to accelerate digital transformation and drive future business growth for your organization.

Medical device manufacturers understand the importance of securing their products to ensure data safety and privacy. However, it is equally as crucial for manufacturers to fortify their internal networks and protect sensitive information to maintain their operational resilience.

Our adaptive organization-wide Security Fabric offers a seamless transition from securing medical devices to enhancing the security of your own internal networks. **By partnering with Fortinet, you will benefit from:**

- Security integrity for medical device R&D and manufacturing.
- Comprehensive, sustainable, and scalable security across cyber-physical IT/OT boundaries for device manufacturers.
- Support for compliance obligations specific to device manufacturers.
- Continuous layered protection for connected mobile medical devices, wearables, telemedicine, and remote health monitoring.

What Makes Fortinet the Right Partner for You?

Fortinet is the preferred cybersecurity partner for large, multi-national organizations in highly complex, highly regulated industries such as manufacturing, government, and banking. This makes us the #1 cybersecurity company in the world: the most deployed, most validated, most patented, and most integrated. When it comes to medical devices, the reasons we stand out from others include our:

- Deep IT/OT security expertise.
- Single, organically developed, inherently secure architecture.
- Airtight SD-WAN connectivity for medical device manufacturers/operators with large data sets/distributed teams.
- Cross-vendor interoperability and visibility.
- Open architectural approach to securing evolving IT infrastructure.

FORTINET

Smart Security for Connected Medical Devices

Securing your medical devices in today's advancing industry atmosphere is imperative. By prioritizing modern cybersecurity, medical device manufacturers can protect private data, ensure device integrity, proactively exceed regulatory standards, and maintain the trust of device users. Partner with Fortinet to fortify your medical device security and enhance the safety and resilience of your devices and business operations.

Click here now to learn more about how Fortinet can help secure your medical devices.

1. Medical Device Cybersecurity: 22 million US health records breached thus far in 2022. GlobalData, July 27, 2022
2. Report: 40% of healthcare organizations hit by WannaCry in past 6 months. Fierce Healthcare, May 29, 2019.
3. Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities. Federal Bureau of Investigation, September 12, 2022.
4. Report names connected medical devices with the biggest cybersecurity risks. Medtech Dive, April 21, 2023.
5. Internet of Medical Things Market Size and Share Analysis, Mordor Intelligence.
6. Medical devices are vital, but vulnerable, IBM, February 27, 2020.