Medigate

Designated Cyber Security Protection Solution for Medical Devices

The Challenge

In recent years, cyber threats have become increasingly sophisticated in terms of attack methods, the degree of damage inflicted, and their ability to circumvent existing security measures. Cyber attacks affect all sectors, however, recently, there has been a dramatic global rise in attacks targeting the healthcare sector.

Cyber criminals aim to attack healthcare service providers to obtain private medical information and disrupt the providers' efficient operation, with the goal of extorting funds from these healthcare institutions. **One of the principal targets of cyber attackers is the range of medical devices in the hands of healthcare service providers.**

There is currently no solution on the market which provides hermetic cyber protection to medical devices, despite the high cost of the devices and their use in the real-time treatment of human medical conditions. This means that the devices at the disposal of healthcare providers are vulnerable to attacks, threatening the continued operation of the healthcare institutions, as well as patient safety and privacy.

Medigate's goal is to provide a comprehensive cyber security solution which will preclude cyber attackers from striking medical equipment.

Types of Cyber Attacks Against Medical Devices

While the methods of cyber attackers have become increasingly sophisticated, they have allowed cyber security experts to identify three primary modes of attack which threaten medical devices.

Ransomware: These attacks directly harm medical devices with the objective of locking them and disabling access. To remove the lockdown, the attackers demand a "ransom" payment which is paid anonymously over the internet using Bitcoin.

Attacks aimed at obtaining private medical information: These attacks enable cyber criminals to obtain personal medical information and patient medical records. Attackers capitalize on the lack of multi-tiered defense of medical devices to extract such information. Alternatively, attackers can use medical equipment as part of their attack vector to reach enterprise servers which house electronic medical records (EMR).

Attacks aimed at disrupting medical treatment: Attacks of this sort have the objective of disrupting sound medical treatment provided to patients, thereby posing a significant health risk. A significant portion of contemporary medical treatments rely on data and measurements that originate from networked medical devices. Cyber attackers can exploit this dependence and tamper with the data and measurements, resulting in the administering of erroneous medical treatment (e.g., incorrect dosage of medication, misdiagnosis of diseases, etc.).

Medigate

Increased Attacks in the Healthcare Sector

These days, most medical devices (Medical IOT) are connected to the communications network of healthcare service providers. The advantage of this is that the multitude of data obtained from such devices can be used to improve the quality and efficacy of patient care. By contrast, the networking of these devices, whether wired or wireless, enables cyber attackers to strike them by means of their accessibility to the communications network.

The statistics regarding this matter are clear, with HIMSS data[1] demonstrating a dramatic increase in the volume of breaches of healthcare service providers. In 2015, 30 healthcare providers were hacked in the United States alone, compared to just 11 breaches in 2013. Beyond the risk posed to human life, these breaches caused $6 billion worth of damage to the U.S. healthcare system in 2016[2].

Nevertheless, the watershed moment for attacks against the healthcare sector occurred in May 2017 with the outbreak of the global WannaCry cyber attack. This massive scale attack exploited weaknesses in the Windows operating system and inserted ransomware which caused a lockdown of the attacked medical device. Although this attack did not exclusively target the healthcare sector, the effects of the attack on the sector were highly significant. For example, in Britain alone over 50 healthcare institutions were attacked, causing the cancellation of medical procedures and the referral of patients to other medical centers.

Increased incidence of cyber attacks in the healthcare sector proves that it is vulnerable and must upgrade its defense systems in general and its defenses of medical devices in particular. With the proliferation of attacks in the sector and the success of the attackers, security experts in the healthcare sector are beginning to understand that the time has come to implement thorough changes in their network defenses and to set this matter as a top priority. Proof of this can be seen in the annual survey of the HIMSS for 2017[3] which asked CIOs in the healthcare sector about their IT priorities. The results were that the top priority was network security, prioritized over other IT issues which are at the very heart of the healthcare industry, such as: patient safety, improved work processes, etc.

The Unique Technological Features of the Healthcare Network

The statistics presented prove that healthcare networks in general, and medical devices in particular, are especially vulnerable to cyber attack. Our analysis has determined that there are several technological reasons for this vulnerability. Identification of these unique technological factors is a critical step which forms the foundation for the development of a targeted solution for the healthcare sector.

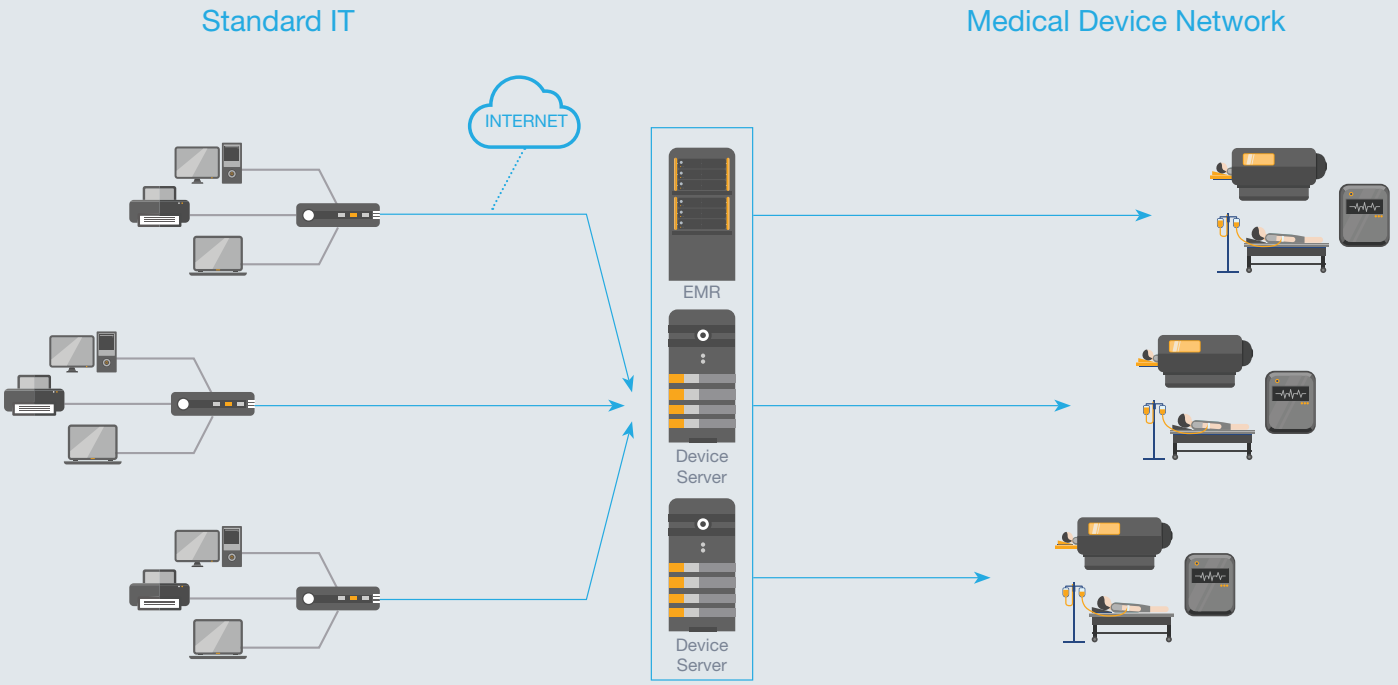
Inherent Connectivity:

A standard healthcare institution's network is comprised of the following sections:

1. **Medical Devices** – Networked medical devices connected to the healthcare institution's network.
2. **Server Tier** – These servers manage the medical devices within the network and store patient medical records on a dedicated server called an EMR (Electronic Medical Record).
3. **IT** – This section is made up of "standard" components such as computers, printers, and laptops used by doctors, nurses, and other medical personnel.

[1] HIMSS 2016 State of the Market
[2] Bloomberg
[3] HIMSS 2017 Cybersecurity Survey

The unique characteristic of the medical network is its inherent connectivity between the Networked Medical Devices and the IT section. This connectivity results, on the one hand, from the medical devices broadcasting data to the Server Tier (and to the EMR specifically), and on the other hand, the IT users accessing those servers to pull patient information which originates from the devices. Moreover, the IT is connected to the internet, since the medical staff needs and depends on internet applications to conduct their work uninterrupted. The result is that there exists a network path connecting the internet to IT, and from there it is only one step away from expensive medical equipment used to treat human beings. This path cannot be disconnected or limited since, at its most basic level, it is essential for the continuous operation of the healthcare institution.



Medical Provider Network Diagram

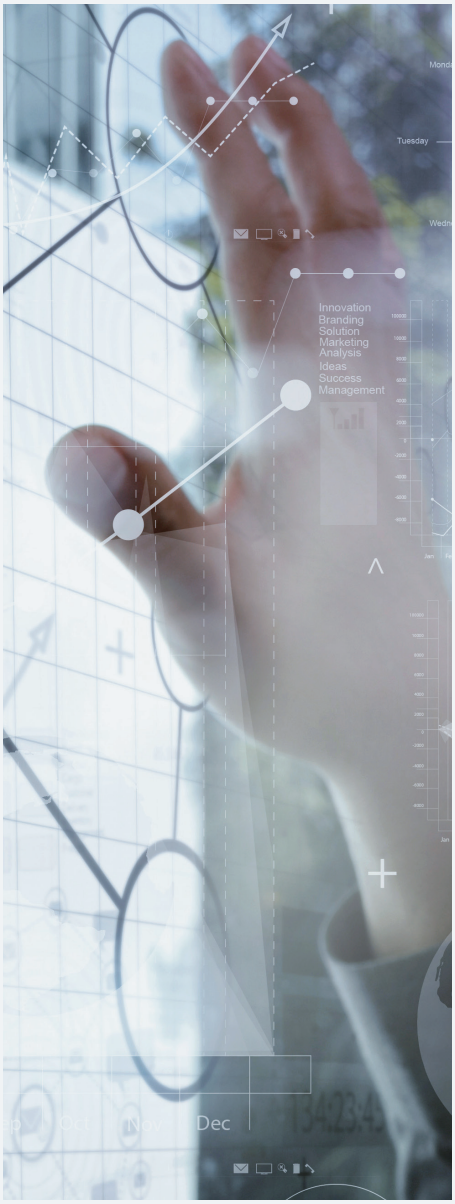
Non-Applicable Defense Paradigm:

Currently, on standard networks it is accepted practice to use a defense strategy which is built on security tiers within the network. The guiding principle here is that it is a given that a singular tier of defense will be breached, therefore the more tiers of protection there are, the probability of a successful attack will diminish. In this context, the security tier of the end points is called End Point Security (EPS) and it is applied by means of periodic program upgrades of the operating systems, and the update of Anti-Virus softwares installed on those same end points. This tier is critical, as it forms the principal and last line of defense of those end points.

In the case of a healthcare network, this paradigm does not work since there are FDA regulations which prevent the editing of programs on medical devices. These regulations were originally designed to ensure that program updates would not adversely affect the functionality of the medical devices, which could potentially endanger patient health and safety. From a cyber defense perspective, these regulations mean that the EPS tier is irrelevant, since anti-virus software cannot be installed and patching cannot be performed when needed. In practice, healthcare networks have extensive equipment and devices running on old operating systems such as Windows XP and Linux, systems which are exposed to dozens of vulnerabilities that have been identified and reported on extensively. This effectively means that their use renders medical equipment even more vulnerable to a breach.

Designated Protocols

The medical devices used in healthcare institutions broadcast data to the Server Tier which manages the devices and collects medical data. This communication is performed by means of designated protocols in the medical sector (Dicom, HL7) and a wide range of designated protocols which are customized to the varying needs of medical device vendors. This mode of communication is highly significant because it means that there exists a medical language which the current security solutions do not analyze and therefore cyber attacks can take place while circumventing these generic security solutions.



Medigate's Unique Solution

Medigate is designing a designated firewall for medical devices, the first ever of its kind. This firewall is built based on the unique characteristics described above and is intented to provide hermetic protection to medical equipment against all types of cyber attacks.

Medigate's firewall will perform two primary roles:

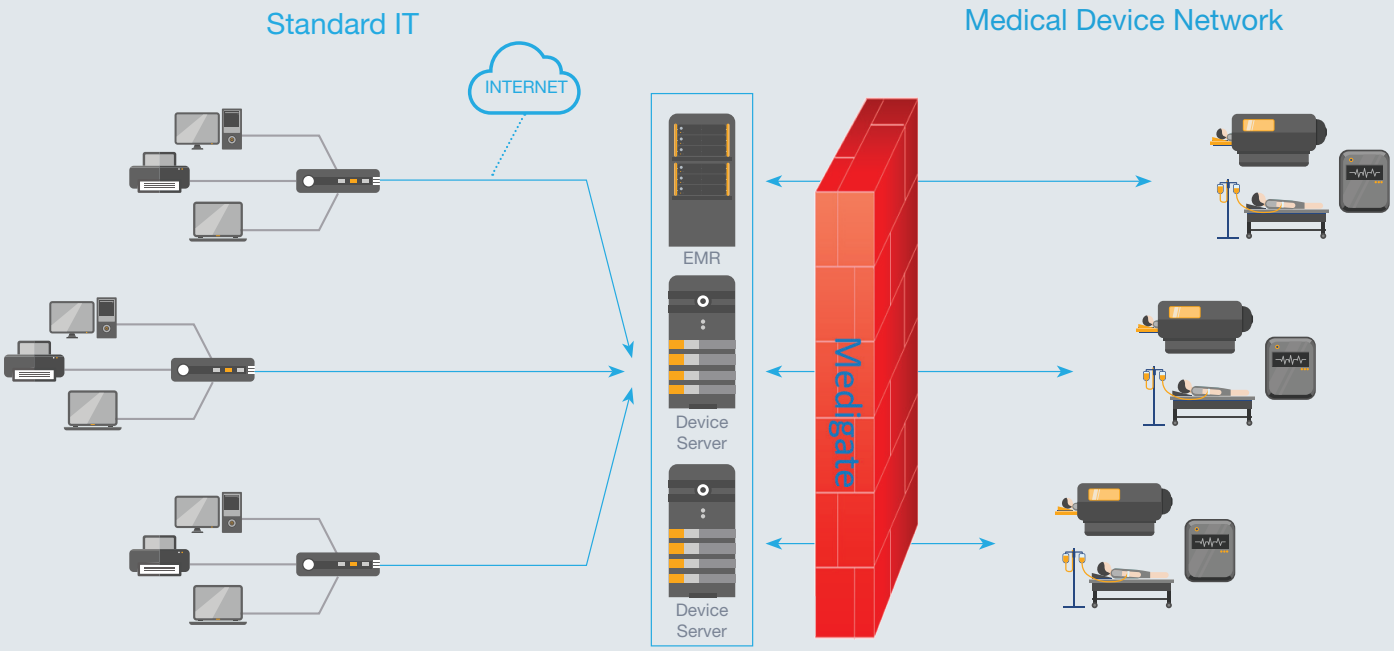
Detection: The product will identify network anomalies specific to the healthcare sector, and will use them to provide real-time alerts about cyber attacks. What makes the product unique in this respect is its ability to automatically learn the make and model of the device (network visibility) and to expose a vast array of network anomalies unique to the healthcare sector. This meticulous analysis of the communication ensures highly credible identification of attacks in real time (and virtually no instances of false positives, which commonly occur among the standard vendors of generic security equipment).

Prevention: The Medigate firewall not only identifies cyber attacks, it also stops them in real time before they can harm medical devices. By utilizing reverse engineering of the communication protocols of the devices, we can block malicious communication from a cyber attack without affecting the operation and efficacy of the medical device. We create an additional, impenetrable line of defense to ward off the attacker on their quest to wreak havoc on the healthcare sector.

Medigate

Medigate's solution is designed to protect healthcare providers by deploying our product on the enterprise level network. Additionally, Medigate's product is designed as an integral Firewall component within a vendor's medical device system (OEM solution).

Enterprise Level Solution



OEM Solution for Medical Device Vendors