SECURING MEDICAL DEVICES & PROTECTING PATIENT CARE

CUSTOMER PROFILE

- Large healthcare provider in the US northwest
- Two dozen hospitals, nearly 3,000 licensed beds
- More than 40,000 employees

CUSTOMER CHALLENGES

- Need for comprehensive asset inventory of medical and unmanaged devices
- Lack of visibility into vulnerabilities in devices, including recall status
- Inability to track the physical location of medical equipment
- Need to monitor device utilization to fine-tune their investments

ARMIS BENEFITS

- **Broader visibility and compliance:** Unified biomedical and unmanaged device discovery and vulnerability identification, providing improved security and compliance
- **Reporting flexibility:** Customized dashboards on a per-user and per-location basis
- **Fast time-to-value:** Deployed the platform in just two hours

Securing medical and unmanaged devices in healthcare

This large healthcare provider's clinical engineering team was responsible for all of the hospital's biomedical devices. They needed a system that could help them not only security medical devices but address tracking devices across facilities and clinics.

The team also lacked a full asset inventory of all their medical devices, as well as visibility into the vulnerabilities and risks in its biomedical devices. Without a clear view of their attack surface, they couldn't take proactive steps to protect the devices, healthcare delivery, or the safety of their sensitive information. A chief concern was the ability to identify FDA classified devices because they are subject to a higher level of scrutiny and security.

Also important was tracking the location of devices. Since most of these are mobile, they are often moved from floor to floor, or even to other facilities. This made it difficult to find equipment when it was needed and to put lost equipment back into service quickly.

In addition, the team wanted a way to monitor device utilization rates so they could right-size their investment in each type of device. For example, if one kind of licensed device was being used too frequently, and another device of the same time wasn't being used at all, the engineering team could balance utilization between the two devices to maximize their value.

How Armis helped

The engineering team was able to deploy Armis quickly, and they immediately started seeing their complete device inventory. The engineering team's leader was surprised by the depth of information Armis was able to provide, and a number of previously unknown and critical risks–including a few surprises:

- FDA classified devices used to access unpermitted URLs, including social networks
- Medical devices transmitting unencrypted patient data over the Internet
- Devices transmitting unencrypted credentials over the internal network
- Devices vulnerable to DNS rebinding, Blueborne, KRACK, and other attacks

The team appreciated the ability to customize the Armis dashboard to suit different use cases depending on user and location. For example, some of the team member's responsibilities focus on asset inventory, while others have to concern themselves with security. And they could also customize the risk factors which helped them in some hospital locations like critical care environments that needed heightened risk awareness than other locations.