ARMIS®

CASE STUDY

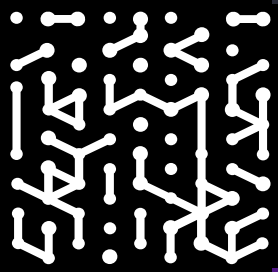
Armis Is More Than a Security Tool for Regional Belgium Hospital

Use cases encompass asset visibility, IoMT discovery, and network operations.

Organization
Sint-Trudo Ziekenhuis

Industry
Healthcare

IT Environment
1250 users, including about 200 physicians
& 200 independent contractors



Introduction

Sint-Trudo Ziekenhuis is a progressive European healthcare facility that prides itself on staying up on the latest medical protocols and treatments. It is equally attentive to its infrastructure, always keeping up on technology advancements and making improvements as required.

Recently, the ICT Director drove an initiative to gain more comprehensive visibility into networked devices and assets as a critical first step toward maintaining compliance with Belgium's strict privacy and security laws. He decided to adopt the agentless Armis platform, which discovered and classified more connected devices than anticipated, including "black-box" Internet of Medical Things (IoMT) equipment.

Armis also helps ensure vendor compliance and enables the operations team monitor the network for anomalies and performance issues.

Sint-Trudo Ziekenhuis is a modern, 320-bed regional healthcare facility located in a Belgium province that offers basic and specialized care.

It is one of four hospitals in the Andreaz healthcare network, which encourages its member facilities to share knowledge, resources, and competencies with the goal of providing over half a million patients with a broad range of high-quality medical services. Sint-Trudo Ziekenhuis has about 1,250 ICT users, including 200 physicians and 200 independent contractors.

Peter De Bruyne joined the organization prior to 2019 as Information and Communications Technology (ICT) Director and board member. He oversees the entire digital IT environment consisting of 1400 devices (PCs, laptops, and smartphones) and numerous on-premises medical devices. Just as the hospital is intent on ensuring advanced healthcare to its patients, it is also in the process of upgrading its infrastructure by incorporating the latest technology tools to support its digital transformation journey.

Discovery is the first step to compliance

The hospital needed a better way to maintain and manage compliance with the ISO 27001 international information security management standard. ISO 27001 certification demonstrates that an organization has systems in place to properly manage and safeguard sensitive personal data, financial information, and intellectual property.

In Belgium, public organizations—such as medical care facilities that perform critical functions for the citizenry—are required by law to be compliant.

Challenges

- Maintaining compliance with European healthcare security & privacy laws
- Gaining full visibility to all connected devices, managed and unmanaged
- Getting insights into risks and vulnerabilities of any connected device, specifically medical devices

To meet these requirements, De Bruyne understood that, in order to apply the right security controls, he and other teams in the organization needed to know exactly what was on the network—and that was his rationale for moving forward with a proof-of-value (PoV) for the Armis platform. He evaluated several other products but, in the end, found that Armis had multiple advantages over its competitors, namely, ease of deployment, user-friendliness, and its ability to collect a comprehensive, rich data set from different sources for all detected devices.

“The data Armis gathers goes beyond just security and vulnerability information, it also includes FDA-compliance status for devices and other information that is relevant to a healthcare operation,” said De Bruyne.

Integrating with the full technology stack

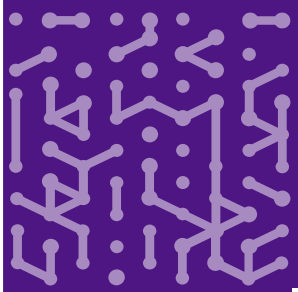
Integrating Armis with existing security and network technologies has been a major focus for the hospital’s technical team. These integrations correlate data from multiple sources across the infrastructure, providing enhanced visibility and enriched actionable information. Currently, Armis is integrated with the hospital’s entire set of Microsoft products.

Among them are Dynamic Host Configuration Protocol (DHCP) for assigning an IP address to devices when they connect to the network, System Center Configuration Manager (SCCM) for managing devices and applications, the Active Directory database to connect users to network resources, and Intune for managing mobile and personal (BYOD) devices.

Armis is also integrated with the backend Cisco local area network and the Cisco wireless network which retrieve information on devices that are connecting to the network, as

Armis Results

- Discovery of nearly double the number of connected assets and devices
- Classification of devices based on rich data sets
- Ensuring compliance accountability of medical equipment vendors
- Providing insights that drive more efficient network operations
- Retirement or containment of legacy systems with outdated security
- Simple deployment and ease of use



well as with the VM ware platform. Down the line, De Bruyne plans to implement a stronger endpoint detection and response (EDR) tool that integrates fully with Armis. He is currently evaluating key players in that space.

Unexpected and welcome benefits

De Bruyne cites the benefits of the Armis deployment in several areas: visibility, asset inventory, operations, and security.
First and foremost, the hospital now has a clear inventory of what is connected to the network and which assets and devices are important to know about. “There are a lot of devices on our network, but not all are relevant. Armis helps us sift through that. That’s a big advantage, so we can drill down to what concerns us most.”

Secondly, in the area of connected medical devices, Armis helps ensure that equipment vendors deliver fully compliant, secure, and future-proof technology. Additionally, it helps the hospital adhere to strict legal requirements around the protection of patient data and other sensitive information.

Thirdly, Armis is being used in security operations to help find root causes for anomalous behaviors, such as under-performance of DHCP and domain name services (DNS). Network issues can potentially impact timely delivery of healthcare services. “Armis showed us that there were some timeouts in certain network segments—something we would not have seen previously. One was discovered during the PoV when we saw performance issues with a heart rate monitor,” related De Bruyne.

Finally, Armis has helped De Bruyne identify and decommission obsolete servers in the data center and other legacy equipment that’s no longer in use. “Armis found a few noncompliant and not fully

“With Armis, we can do operational drill-downs and root cause analysis. It is more than just a security tool for us.”

Peter De Bruyne
ICT Director, Sint-Trudo Ziekenhuis

secured legacy servers in the laboratory and other medical facilities. It's a danger if these devices with outdated security are still on the network. Armis helps us do better housekeeping," he noted.

Forging a lasting relationship with Armis

When De Bruyne made his decision to adopt Armis, he was struck by how the company stands by its customers throughout the sales process and especially beyond. "The relationship got off to a great start and remains positive. With the regular calls our people have with Armis specialists, we feel very well supported and have continual follow-up. Armis wants to make sure we get full value from the platform, and we really appreciate that. With other vendors, this is rarely the case," observed De Bruyne.

He added that their professional services and security partner collaborates closely with Armis, providing additional assurance and a sense of confidence as the hospital continues on its digital transformation path.