ARMIS

GIG CYMRU NHS WALES
Bwrdd Iechyd Prifysgol Cwm Taf Morgannwg University Health Board

CASE STUDY

UK Healthcare System Relies on Armis to Discover, Segment, and Secure Essential Medical Devices, IoT, and Legacy Assets

The Challenge

- Lack of visibility into traffic flows in the environment
- Securing and segmenting mission-critical legacy medical devices
- Identifying, prioritizing, and remediating a backlog of vulnerabilities in the environment, particularly IoT assets
- Complying with UK government security standards, including NIS2 Directive and GDPR

The Solution

- Deployed Armis Centrix™ for Medical Device Security
- Installed three Armis collectors, one at each of the main hospitals
- Configured Armis Centrix™ for VIPR to help prioritize vulnerabilities
- Integrated with Cisco Wireless LAN controllers, DHP servers, and Microsoft System Center Configuration Manager (SCCM)
- Integrated Armis with Cisco Identity Services Engine (ISE), Microsoft Defender, SolarWinds, and server antivirus solutions
- Implemented automation to act on vulnerabilities

The Results

- Provided visibility into how traffic and data flow across the environment
- Enabled segmentation of departments and legacy servers
- Deployed a third-party patching solution based on data from Armis
- Established a plan to remediate vulnerabilities in the endpoint estate
- Set up passive monitoring of the environment to comply with regulations
- Support compliance and audit reporting for key directives like NIS2 and GDPR

Industry Healthcare

Location Wales, UK

Number of employees 14000

Armis Centrix™ for Medical Device Security

Armis Centrix™ for VIPR - Prioritization and Remediation

Background

The Cwm Taf Morgannwg (CTM) University Health Board is the local health board of the National Health Service (NHS) of South Wales. It serves about a half million people in southern Wales with three main hospitals, providing a variety of healthcare services. Thomas Evans, head of cybersecurity operations, oversees a team of six full-time staff. The hospital's environment includes conventional IT assets such as computers, laptops, mobile devices, switches, access points, and firewalls, as well as medical devices, cameras, IoT assets, and a few vehicles, including a van that performs endoscopy scanning.

The Challenge

The biggest challenge Evans faced in securing and protecting the environment was a lack of visibility into traffic flows and assets on the network. In particular, he was concerned about legacy medical devices and IoT assets that could have unidentified vulnerabilities. "You can't start fixing stuff or prioritizing what to remediate until you know what you've got," Evans pointed out.

Some of the organization's medical devices that are critical to hospital operations and delivery of medical care run on legacy operating systems that cannot be updated at the moment. Evans needed a way to get visibility into these EOL and EOS assets in order to get a handle on potential vulnerabilities

"I have only positive things to say about Armis. It gives us a level of detail and data that we didn't have before. I don't think there's anybody here that would question the value Armis brings to this organization. It's all been positive."

Thomas Evans
Head of Cybersecurity Operations, The Cwm Taf Morgannwg University Health Board

and make decisions about whether these assets need to be remediated with patching or updates. Having visibility to understand what these assets are doing on the network and being able to segment them is important to securing the environment and ensuring continuity of care.

The Solution

After a successful six-month POV, Armis Centrix™ for Medical Device Security was deployed at all three hospitals with the help of the Armis team. Evans noted that Armis was one of the easiest systems he's ever rolled out. Armis Centrix™ for VIPR – Prioritization and Remediation was also deployed to help with the prioritization and remediation of newly identified vulnerabilities.

"I simply installed the collector and integrated the software—and Armis did the rest. It's quite intuitive and straightforward to use," Evans remarked. He shared that what made Armis stand out from other providers was how comprehensive the asset catalog and data were in the backend database. He also appreciates how Armis sits on the network and is agentless. It provides passive monitoring of the environment, which is needed for compliance with UK security directives.

The Results

Armis identified 65,000 to 70,000 IP-connected assets, including medical devices and some TVs, game consoles, and even vehicles. "Armis gave us really good visibility over the medical devices talking on our network. It identified a few that we didn't know were there and allowed us to resolve or remove them," Evans explained.

Using the network connection reports in Armis, Evans drew up a process to segment servers with legacy operating systems to isolate them from other networks. He is also using Armis data to segment the hospital's departments, starting with the most critical one: the blood bank. His plan is to map out the department's most critical devices, such as blood analyzers, and use Armis to see exactly what they do on the network, building the segmentation out from there. After mapping out and segmenting the blood bank department, he will move on to intensive care and radiology.

Another area where Armis is providing value is compliance with the NIS2 Directive and GDPR. Each year a government-guided cyber assessment is performed by organizations or a third-party auditor to check for compliance. "Getting Armis has checked off one of the biggest red marks for us on the audit. It's a massive help," shared Evans.

Armis has empowered Evans to formulate a plan to tackle the significant backlog of vulnerabilities in the hospital's endpoint estate. The data helped him make the economic case for bringing in a third-party patching solution, taking a big burden off his stretched-thin team.

"Armis shows us the vulnerabilities we have with reports and data, so our teams can go in and fix the issues. There's value for all teams involved," he remarked. He is in the process of setting up automations in Armis to take action against risky or unapproved devices. "Having Armis act on our behalf instead of having to analyze everything at a granular level will be a massive time saver," he said.

Evans and his team have integrated Armis with numerous systems, including Cisco WLAN, DHCP servers, SCCM, SolarWinds IT management and monitoring, and server antivirus solutions. He also plans to integrate Armis with Microsoft Defender and Cisco Identity Server Engine (Cisco ISE). His long-term goal is to leverage Armis for collecting details on medical device connections and traffic activity, including identification of ports and IP addresses. This will help Evans and his team build baselines for what is legitimate asset behavior.

Looking forward, Evans mentioned that he will use Armis to provide lists of vulnerable assets to the departments so they each have the evidence they need to put a case forward for updating their systems or assets when the next budget cycle comes around. “I can foresee this will be a big part of the value we get from Armis in the near future,” he said.

650
servers identified

10,000
endpoints secured

65,000 to 70,000
IP-connected assets, including medical devices, discovered

ARMIS®

1.888.452.4011
www.armis.com

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization’s cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.