ARMIS

NHS
The Princess Alexandra Hospital
NHS Trust

CASE STUDY

Armis Secures Hospital Undergoing Digital Transformation

The Challenge

- Secure the expanding attack surface from malware and cyber threats
- Identify and segment legacy IoT and IoMT devices
- Automate asset discovery and vulnerability management

The Solution

- Deployed Armis Centrix™ across three hospitals and one administrative centre
- Connected the Electrical and Biomedical Engineering (EBME) team with the IT team through a single-pane-of-glass dashboard
- Provided visibility into IT, IoT, and IoMT assets, both managed and unmanaged
- Integrated with existing products in the environment

The Results

- Automated asset discovery and vulnerability management
- Improved operational efficiency by reducing time spent on manual tasks
- Increased security posture and decreased MTTR
- Prevented a device connecting to a known malicious domain from spreading malware

Industry: Healthcare

Location: Harlow, Essex, UK

Size: Approximately 4,500 employees

Armis Centrix™ for Medical Device Security

Background

Princess Alexandra Hospital NHS Trust is a general hospital with 420+ beds located in Harlow, Essex, UK. Its facilities include three hospitals and one administrative centre that provide a broad spectrum of patient care—emergency response, specialised outpatient care, surgical services, maternity care, and more—to approximately 350,000 to 500,000 residents in the surrounding community.

With a background in the private sector, Jeffrey Wood, deputy director of information and communication technology, is working on a 2030 vision to transform the organisation into one of the most digitally advanced public healthcare trusts in the UK. Among his initiatives are a virtual holographic receptionist that speaks six languages, cloud telephony, an electronic health record system, and improvements in cyber resilience and security.

The Challenge

The healthcare industry and its data are a top target of cyberattacks. It only takes one incident to have devastating effects on both patients and the hospital.

© Copyright Armis 2025

"The proof of concept was invaluable in allowing us to understand what the issues and problems were. You need to be aware of your problems before you can even start looking at security areas to plug. Cybersecurity is constantly changing, and it's a priority to understand where the gaps are in the attack surface."

—Jeffrey Wood
Deputy Director of ICT,
Princess Alexandra Hospital
NHS Trust

With more and more internet-connected equipment being added at Princess Alexandra Hospital, Wood was concerned about the growing attack surface. He recognised the need to have visibility into everything that could be an attack vector for hackers. The medical equipment and every piece of new technology—from the virtual receptionist to new IoT lockers—create additional risk. It was also a challenge for his team to keep up with patching on legacy medical equipment, some of which still operate on Windows XP, Linux, and Unix.

"Cybersecurity is constantly changing, and it's a priority to understand where the gaps are. We are well aware that medical records are some of the most sought-after assets by hackers, and it's important for us to consider those risks every time we take on a new technology," Wood explained.

To that end, he invited Armis to design and run a proof of concept (POC) to expose any security gaps. The POC was eye-opening for the security team, uncovering a vast amount of equipment onsite that they were unaware of, including gaming stations, smart automobiles, and IoT equipment like coffee machines and vending machines. As Wood pointed out, while the presence of these less secure devices is not problematic in itself, it is critical to segregate them from the corporate network to prevent negative consequences of potential compromise that could impact hospital operations and patient care delivery.

The Solution

The hospital deployed Armis Centrix™ for a three-month POC to monitor, track, and investigate various devices in its environment: IT infrastructure, picture archiving and communication systems (PACs) used for medical imaging, laptops, Android and iOS mobile devices, IoT, and IoMT. The hospital's Infrastructure Engineer, Matt Formela, pointed out how Armis created a bridge between the Electronic and Biomedical Engineering (EBME) team and the IT department, which previously did not have any visibility into medical devices.

Armis Centrix™ integrates with products already in use within the hospital's environment, enabling it to consolidate and verify information. To align with the UK's National Health Service (NHS) standards, Armis also provides Data Security and Protection Toolkit (DSPT) dashboards that get updated as compliance changes.

The Results

Armis has improved operational efficiency by automating asset discovery and vulnerability management, which allows the hospital's IT and security teams to gain visibility into the device landscape, better understand device behaviour, and focus on proactive threat management rather than on time-consuming manual tasks. Woods and his team use Armis Centrix™ to quickly act on all CareCert alerts generated by NHS England Digital by tracking devices that need patching. Moreover, by cross-checking alerts against the Microsoft Defender for Endpoint database Armis eliminates false positives and reduces alert fatigue.

Armis provides the hospital's security team with a single pane of glass for viewing all connected assets, both managed and unmanaged. This enables the team to pinpoint the exact location of devices that require manual updates. Armis has strengthened the hospital's security posture by quickly identifying vulnerable devices and reducing Mean Time to Resolution (MTTR).

"We use Armis to monitor, track, and investigate various devices for informational purposes and cybersecurity investigations," pointed out Wood.

© Copyright Armis 2025

"We have a clear vision of where and when devices attempt to connect to malicious websites and can act on that in a timely manner. This visibility allows us to put pressure on software developers who still use legacy protocols."

—Matt Formela
Infrastructure Engineer,
Princess Alexandra Hospital
NHS Trust

In addition, he noted that, within an NHS trust like Princess Alexandra Hospital, his team frequently shares security data with external auditors, the performance finance committee, and the executive board. "The Armis Centrix™ dashboards," he remarked, "are a great means to pull out that information and present it in an easy way to those teams."

Recently, Armis detected a device that was connecting to a malicious domain known for distributing Pikabot malware. Armis data was used to validate the connection, swiftly isolate the device, and set up firewall rules to block any and all connections to the offending domain, preventing a major outage.

Next up, Wood is looking at how Armis could potentially streamline clinical workflows. "We're still in the early stages," said Wood. "As we move in that direction, we are starting to work on ensuring that critical medical devices are updated with their latest software patches and, when Armis allows the 'recall' feature for the European market, we will utilise that as well."

Wood acknowledged that cultivating a close partnership with Armis, not only enabled a seamless deployment but is also helping the hospital get the most out of the platform for its specific environment. "One of the things that was important to us during the procurement process was finding a partner that would support us during the early stages. Armis has been there to help us develop and use the system as time has gone on—and that's the key to a successful implementation," concluded Wood.

3,500
iPads identified across 3 hospitals

5,000
laptops and desktops secured and protected

2x
the amount of equipment added to the hospital's environment since running the POC

ARMIS®

Armis, the cyber exposure management & security company, protects the 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.

1.888.452.4011
www.armis.com