ARMIS®

THE MATER HOSPITAL

CASE STUDY

Premier Irish Healthcare Provider Closes Security Gaps

Hospital Group CIO deploys Armis to facilitate better patient care through informed decision-making

Customer profile

Top Irish provider of innovative medical care to its patients. Mater is a level 4 teaching hospital that provides a range of frontline and specialist services on a regional and national level.

Industry

Healthcare

IT environment

Network-connected endpoint assets, along with third-party biomedical equipment from various suppliers used by 4,300 employees.

Introduction

Mater Misericordiae University Hospital in Dublin, Ireland is known nationwide as a top provider of innovative medical care to its patients. The hospital's Group CIO with the hospital CISO realized that comprehensive security and network visibility was essential to achieving the organization's mission. To fulfill the organization's commitment to excellence, quality, and accountability, the CISO implemented Armis as a way to help clinicians and other hospital workers to swiftly, freely, and securely access the information they need to make the right treatment decisions for patients. Armis also provides broad visibility to all network-connected assets, including third-party equipment, and, by doing so, helps lower overall risk and maintain compliance with E.U. regulations.

Founded in 1861 by the Sisters of Mercy, Mater Misericordiae University Hospital (Mater Hospital) in Dublin, Ireland is a levelfour acute care teaching hospital and is part of the Ireland East Hospital Group. The hospital provides frontline and specialized patient care for both the immediate area and at a regional and national level. It serves a population of roughly 1.5 million and has an inpatient bed count of approximately 712.

The busy healthcare facility employs approximately 4,300 employees and is funded by the state. Mater Hospital is renowned as a national center for multiple surgical and therapeutic interventions and treatments: heart surgery, heart and lung transplants, pulmonary hypertension, spinal injuries, rare diseases, forensic and postmortem imaging, and deep brain stimulation, among others.

As chief information officer (CIO) for the entire Ireland East Hospital Group, Dr. Michael Connolly is well aware that healthcare is a risky business. His mission is to ensure that the information that is available to clinicians is up to date, relevant, and pertinent to every patient's care requirement.

"Clinicians are dependent on the patient data being available to them so that they can make the best decisions. We take that incredibly seriously, and we are passionate about our involvement during the patient care journey," says Connolly. "Anything that interferes with the flow of information to inform those decisions, we would consider a risk."

How cybersecurity can potentially impact healthcare delivery

With that in mind, Connolly undertook an assessment of gaps in the organization's existing security defenses. He and his team quickly discovered that they had some major blind spots: they had no idea what assets were connecting to the network, the patch status of various assets, or specific device vulnerabilities.

"We had no visibility and were blissfully ignorant," points out Connolly. "We lacked threat and vulnerability enumeration for our vast estate of assets, which were running multiple versions of operating systems and had different configurations. We knew that if we didn't have insights into the network, patients could suffer—and we simply could not afford to take that risk."

Armis: One solution, many uses

As a leading healthcare provider in Ireland, Mater Hospital always partners with best-of-breed vendors. Connolly evaluated and selected Armis, as he believed it fit that profile. He found that Armis was well-tested and could offer the hospital the dual functions of cybersecurity protection and asset visibility. He describes the Armis solution as "two products for the price of one."

Armis met the hospital's stringent and highly specific requirements. After deployment, Connolly says that he and his team gained immediate visibility into the number and types of assets that were connected to the corporate network, the guest network, and the wireless network. To Connolly's surprise, Armis even discovered an automobile connected to the publicly accessible guest network. Since Armis provides full asset context, including IP addresses, media access control (MAC) addresses, type, location, and owner, the Information Security team can rapidly pinpoint problematic assets and then address any issues, such as outdated patching or vulnerabilities. This data can also be used for future asset audits.

Connolly and his team have already integrated Armis with Microsoft Active Directory and Microsoft Endpoint Configuration Manager, which helps them manage Microsoft Windows endpoints, including installation of updates and application of security patches. Next on the agenda are integrations with the organization's security

Challenges

- Closing security gaps and improving overall risk and security posture
- Getting a better handle on third-party and supply chain assets connecting to the network
- Uncovering vulnerabilities and determining the security status of all assets
- Ensuring that clinicians have fast and easy access to the relevant data that helps them provide the best possible healthcare for patients

operations center (SOC) and security information and event management (SIEM) solutions. Integrating Armis's contextual asset inventory into these technologies will significantly reduce incident investigation time by having all critical security data available in a single location.

Connolly notes that Armis has successfully helped identify gaps in the organization's security posture by enabling network asset risk evaluation (for both hardware and software) and software version enumeration. This applies to third-party supply chain assets, as well as in-house assets.

Armis holds third parties accountable for maintaining assets

As Connolly points out, a significant eye-opening outcome of the Armis deployment was discovering the state of disrepair of some of the third-party and supply chain equipment that is connected to the hospital's network. Prior to implementing Armis, his team had no visibility to these assets at all. Armis helped the team find equipment that should have been maintained but had not been and even third-party assets that were infected and connected to command-and-control centers used by attackers for propagating malware.

"Armis gives us precision-based evidence so we can deal with third-party suppliers who are connected to our infrastructure and hold them accountable. Now we can tell them what state their equipment is in and what needs to be done to bring the equipment into compliance with our contractual agreements. All of this helps make our environment a safer place from a cybersecurity perspective," asserts Connolly.

Armis also provides valuable asset utilization and software use information, which the hospital leverages for resource allocation and to maximize service usage efficiency.

As a healthcare provider, Mater Hospital is governed by the EU NIS Directive, whose aim is to establish a common level of security for network and information systems across the European Union. If, for example, a healthcare provider was the victim of a cyberattack, the organization would be obliged to report the incident and implement the required mitigations. The organization could potentially be held liable and be fined for disruption of essential services. The directive also requires organizations to have a complete asset inventory. Armis was able to bring Mater Hospital into compliance with minimal effort.

"Armis gives us precision-based evidence so we can deal with third-party suppliers who are connected to our infrastructure and hold them accountable. Now we can tell them what state their equipment is in and what needs to be done to bring the equipment into compliance with our contractual agreements. All of this helps make our environment a safer place from a cybersecurity perspective."

Dr. Michael Connolly
Chief Information Officer (CIO)
Mater Misericordiae
University Hospital

Armis is indispensable to hospital security and risk management

Connolly views Armis as an essential addition to the organization's "security defense shield," as it helps prevent disruption in operations and instills greater peace of mind in everyone at Mater Hospital.

"Metrics and accountability are key to understanding how to protect the hospital's network, and Armis has a major role in making the relevant data available to us in an easy-to-access manner," underscores Connolly. "It has definitely filled in the gaps in our security arsenal by uncovering risks we never knew about previously. At first, I thought Armis was a nice-to-have, but now it's become an integral part of our cyber defense."

Armis is instrumental in supporting superior patient healthcare at Mater Hospital. "Armis does exactly what it says it does. It was simple to implement, and it is easy to use. Above all, Armis quickly collects the data we need to help us make informed decisions on how to deliver the best possible treatments to our patients," emphasizes Connolly.

In the near future, Connolly and his team will be leveraging Armis to accelerate incident response times by increasing their ability to discover and measure information security risks and further harden medical asset network interactions and access.

"As a national trauma center and the largest healthcare providers in Ireland, we're looked upon as a leader. One of my goals is to show our other 11 hospitals how Armis can help them become more proactive and progressive in keeping their networks and assets secure," asserts Connolly.

Armis Results

- Immediate and complete visibility to corporate, guest, and third-party assets
- Improved oversight over biomedical asset security status and updates
- Measurable risk reduction through enforceable supply chain accountability
- Maintaining compliance with European Union cybersecurity directives
- Delivery of optimum healthcare to patients based on decisions informed by data

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

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 safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial