Customer profile

Medical equipment and technology provider.

Industry

Manufacturing

IT environment

Global locations, with close to 3,000 employees worldwide and as many as 20,000 network-connected devices of all types.

PIONEERING MEDICAL TECHNOLOGY AND MANUFACTURING COMPANY ACHIEVES BROAD AND DEEP VISIBILITY

Armis enables security and IT team to build an accurate and complete asset inventory and accelerate vulnerability management

This rapidly growing medical technology and manufacturing company, with mergers and acquisitions (M&As) at the core of its expansion and innovation strategy, implemented Armis to create a comprehensive asset inventory in alignment with NIST CSF standards. The agentless solution identified nearly all network-connected IT, IoT, and OT devices, while also significantly improving vulnerability management and providing enriched data that is easily accessible from a central dashboard.

CONNECT WITH US

As an innovation trailblazer, the organization's key security concerns revolve around protecting intellectual property (IP) and source code for their products and keeping day-to-day operational data safe. The security engineer and his team are dedicated to this mission. The security team is engaged with the business in multiple facets of cybersecurity: IT and OT, product lifecycle management, software development, R&D for emerging technologies, and compliance to industry and other regulatory mandates. The security team collaborates closely with the 60-person IT team to keep things running smoothly and efficiently.

In search of the right asset inventory solution

The security engineer and his team follow the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and look to the Purdue industrial control system (ICS) security model for additional guidance. The NIST CSF prescribes a complete physical and software asset inventory and an understanding of the communication and data flows between devices. These were the biggest security challenges the security engineer faced—until he rediscovered Armis.

"We lacked a cohesive understanding of where everything was located, what our devices were doing, and what they were talking to. Asset discovery was a challenge, as was vulnerability management," he says. As he points out, in an environment that has IT, IoT, and OT devices, not everything is "agent able."

Already familiar with Armis, the security engineer decided to revisit the solution and determine whether it was a viable fit. After assessing it against other vendors and performing a proof of value (PoV) at the main office, he and his team had all the evidence they needed. Armis was the product they were looking for.

Asset discovery and vulnerability management go hand in hand

Setup was remarkably easy and fast, and the product provided useful data immediately. For this organization, one of the most valuable capabilities of Armis is that it goes beyond agent-based solutions. It provides passive, agentless monitoring, which is critical because traditional security agents cannot be used on certain devices, such as cameras, mobile phones, televisions, and other IoT and OT systems found at the organization. The security engineer can now say with certainty that Armis has been able to keep the number of unidentifiable devices to a bare minimum.

"When these types of devices are unpatched, they represent the possibility of an exposed vulnerability on your network. And, if you are not aware that they exist, cybercriminals can have a field day camping out on such devices, which have minimal intelligence," he observes. With Armis, he and his team can detect these devices and swiftly take action to patch and update them. As an added plus, Armis enables them to mark their progress and see the results of their efforts.

Challenges

- Getting a better handle on all devices: IT, OT, and IoT
- Creating more a complete asset inventory following NIST CSF standards
- Gaining deeper, more comprehensive insights into the entire environment, including vulnerabilities
- Understanding data flows and communication between devices

"Now that we have Armis, we can even look at end-of-life (EOL) operating systems. Let's be honest, everyone has some degree of 'technical debt' in their environment," notes the security engineer.

Armis can also scale and grow with the organization through its many M&As. In fact, it is one of the first solutions that the security engineer and his team employ when folding in a new company's network post-acquisition. "Even before our firewalls are deployed, we use Armis sensors to give us a visible spectrum of what's in the environment and what our potential risks are. It's tremendously valuable in that context," he affirms.

A centralized dashboard brings it all together

The data enrichment from integrations with the tools the security engineer and his team already leverage has proved invaluable. Current integrations include a popular cloud computing platform, a mobile device and mobile application management solution, and other network and endpoint management tools. These integrations enhance the team's ability to correlate data from multiple sources and derive better insights. For example, as the security engineer notes, all of those data points provide a view into software configurations so they can monitor configuration drift over time and see where things have changed or need to change.

Additionally, not having to switch between multiple management consoles is a major advantage. Armis consolidates all data into a single, easily accessible dashboard.

For the security engineer and his team, Armis's vulnerability management capability serves as a system of checks and balances, helping them prioritize what to patch and when. "For example, we use the query language to check on printers that are vulnerable. When we discover those, we send the spreadsheet to the site administrators and give them their marching orders on what they need to resolve. Once they have applied the patches, the printers drop off the list because they show up as remediated. This provides us with validation," he explains.

Making the most out of their investment

Well aware of the limitations on his staff's time, the security engineer opted to sign up for Armis as a service, which provides the organization with top-tier support for rapid issue resolution, access to seasoned experts for help with customizations and other enhancements, and opportunities for training.

"It was a logical choice to have Armis professionals guiding us. We've had a ton of ideas come out of our weekly meetings with the Armis team, such as how to do things better and how to look at the data differently," remarks the security engineer. "They are incredibly responsive, and we've derived a lot of value from an educational perspective."

He has leveraged the service to train the technical staff on how to create structured queries so they can ask the right questions and zero in on the answers more quickly. Additionally, they have learned how to customize dashboards for specific use cases.

> "From a visionary perspective, Armis has it all. It's doing exactly what it's designed to do."
>
> **Security Engineer**
> **Manufacturing**

The Armis as a service team also makes it a regular practice to keep the security engineer and his team up to date on new features and functions that are slated for release.

“Working with a vendor has to feel like a partnership. It has to be a continual dialog. It’s about working together to solve problems. With Armis, I’ve never felt like I’ve been left holding the bag, waiting for an answer,” he says.

Armis empowers users

Both the security staff and the IT team have evolved into Armis power users, largely as result of the user-friendly interface layered over a robust architecture.

“Armis is obviously listening to people and building in what they are asking for. The new dashboard is a great example. From a user experience perspective, it’s not hard at all to find what you’re looking for. You don’t have to go 15 layers deep. Most of our team members can find answers on their own,” asserts the security engineer.

He cites an example where he had a meeting with his CIO and was able to immediately access and report on highly specific data about browser usage. “I was able to show my CIO which browser version a certain person was using. Once I learned the syntax of the Armis query language, it was easy to build the queries we needed to get our questions answered,” he explains.

“From a visionary perspective, Armis has it all. It’s doing exactly what it’s designed to do,” concludes the security engineer.

Armis Results

- Nearly 100% device discovery due to agentless, passive monitoring, which covers all device types
- Identification of unpatched or out-of-date devices for more accurate and timely vulnerability management
- Customizable reporting and a user-friendly, centralized dashboard
- Integrations with current tools providing an enriched data set for improved correlation and actionable information

About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

1.888.452.4011 | armis.com

20220902-1

ARMIS