Customer Profile

Equipment Manufacturer

Industry

Industrial manufacturing

IT environment

Over 10,000 employees worldwide and thousands of devices on IT and OT network

Global Industrial Equipment Manufacturer Secures OT Environment and Protects Operational Continuity

Armis removes the “black box” of uncertainty about what is on the network

This manufacturer of heavy equipment has evolved its production capabilities increasingly into digital processes. With a massive labor force of skilled engineers and production workers, maintaining productivity on the shop floor is a top priority. Armis helped the manufacturer segment, secure, and redesign the OT network with confidence and efficiency, reducing the attack surface and preventing lateral threat movement from potentially hindering productivity.

The company is based in the northeastern US and is a global manufacture of heavy equipment.

The vice president of cyber security/CISO is a 20-year veteran of the company. He works closely with another longtime employee, the information security engineer, who manages security operations. Though they've never had any incidents and have confidently managed the organization's IT stack and devices, they began to express concern over the security of operational technology (OT) devices on the production floor. Driven by a continually evolving manufacturing process, the company has been putting more intelligence into digital production processes, leading to more assets that fall outside of the typical IT category—such as giant laser cutters and plasma cutters that require access to engineering files in order to cut pieces of metal. As the CISO puts it, he and his team did not "have a good picture" of what devices were actually on the OT network.

Concerns over business continuity drive Armis deployment

"A big part of what we do is actually being able to make product and run our shop floor," the CISO stated. If an attacker were to target the company, he noted, it would most likely be a ransomware or denial-of-service (DoS) attack in the OT environment. "It would be very costly for us," he explained. "The biggest thing that we're looking to do is to maintain productivity," he stated. "We could see where potentially this was going, and we just wanted to get ahead of it. That's where Armis came in."

The CISO pointed out that people are the organization's biggest security challenge. As such, the security team has already been spending "a lot of time" on phishing training. He described the kind of cyberattack that most concerned him and how Armis would be used to mitigate the damage.

"The typical attack vector might be a user who gets phished and gives up their password, and then they get tricked into giving out their multi-factor authentication. The

Challenges

- Gaining visibility into business-critical OT assets in the environment
- Reducing overall risk profile and improving security maturity
- Gaining visibility into network traffic
- Reducing fear, uncertainty, and doubt (FUD)

attacker gets a foothold into our network, or maybe there's a piece of malware that, for some reason, we didn't catch, and they get a foothold. Now they're looking to do some damage…by moving laterally in the network."

The CISO was looking for a way to monitor unusual traffic going into the OT network and trace it back to the initial source. After experiencing other asset inventory tools first-hand and seeing that they only showed that devices were present on the network and little else, he found that the agentless Armis platform provided so much more capability and was a great fit for the OT environment.

Passive monitoring, with detail, differentiates Armis from other asset inventory tools

The team started out with a two-month Armis proof of value (PoV) before fully deploying the platform. The time to value was immediate. The information security engineer recalled that the PoV was first implemented at two of the company's larger sites. "We saw PlayStations and Xboxes pop up, usually on a Friday, and then get shut off on a Sunday. Before we would not have known that unless we physically saw that happen," he said.

Passive monitoring is one of the capabilities the CISO most appreciates about Armis. "Our traditional inventory tools are active scanners. You run the scanner, it goes out, and, if the device is there, it'll answer back. [With Armis], it's actually looking at network traffic to identify the devices. So, even if we're not running a scan, we feel comfortable that if a device is on [the network] at some point, we'll see it," said the CISO.

Another point of differentiation is the level of detailed data that Armis provides. "With our other tools, we knew we had the devices—we just didn't really know what they were… instead of saying, 'Hey, this is a generic Linux device,' Armis will say, 'This is a Siemens PLC.' It actually lets us know what it is, and that helps us identify our risk."

Armis Results

- Higher level of comfort and awareness of what is on the network
- Reduced attack surface
- Easier to segment and secure the network
- Automated alerting to any unusual traffic
- Assurance of business continuity

Armis helps the team segment the network and reduce the attack surface

With his long history at the company, the CISO has seen the evolution of the company's business over time. "Back in the day, we were small. We started as a holding company," he noted. Over the years, the company bought a lot of businesses, leaving the networks as is, for the most part.

"As we're starting to make reinvestment in the networks, we're actually able to do redesigns and we're able to get better segmentation. Now we segregate our shop floor devices or production devices into a more secure network. For example, we put them behind a firewall," said the CISO. With the visibility provided by Armis, he can easily see where in the network these devices are sitting and can move them to where they need to be, and this has provided the CISO and the security team with a greater sense of reassurance and control.

"I was really anxious about not knowing what was out there. I think that's always a big worry for people in cyber space. It was almost like there was a black box... and we were wondering 'what's going on in there?'" said the CISO. That discomfort has been greatly alleviated, thanks to Armis. "I feel confident that, at any point, if I see... something unusual, I can jump into Armis and figure out what the device is, which switch port it's connected to, and, where it physically sits."

Developing the "gold image" to add new devices efficiently and securely

Sony PlayStations and Microsoft Xboxes are not a big concern for the CISO, since they typically have regular updates for their gaming platform. It's devices like Raspberry Pis that operate on Linux platforms that are more of an issue. Raspberry Pis are high-performance small single-board computers (SBCs) about the size of a credit card that are used for industrial applications as

well as for consumer products. The information security engineer says that the security team has created what they call “the gold image” to manage these types of devices more efficiently.

“When someone brings in a new Raspberry Pi or new widget, they’re able to use what we call a ‘gold image.’ Knowing what types of vulnerabilities have already been discovered by the Armis platform for similar devices, they’re able to go in and bring the new Raspberry Pis up to a certain level of security, using the snapshot of the gold image that was already developed,” said the information security engineer. He noted the team also uses the gold image concept for adding new cell phones.

Moving into the fine-tuning phase

Although the CISO’s main concern is cybersecurity, he noted that the information security engineer has been working closely with the manufacturing engineers on putting Armis to use from an operational standpoint. The engineers have shown a high level of interest in using Armis. The CISO pointed out that they will derive significant value from the platform well, in terms of being able to see, manage, and configure their devices more efficiently.

With the Armis implementation still being relatively new, there’s still optimization to be done: refining alerts, setting policies, and integrating the Armis platform with other tools. Although the team is receiving more alerts now than ever before, the CISO views this as a positive development. “The level of comfort we now have with the visibility Armis provides overrides any additional work we might have to deal with,” he shared. He expects the workload to get progressively easier as they set up automations and further tune Armis to their needs. “We’re receiving the data, and that’s the big thing,” he asserted.

“The level of comfort we now have with the visibility Armis provides overrides any additional work we might have to deal with. We’re receiving the data, and that’s the big thing.”

CISO
Industrial Manufacturing

About Armis

Armis is the leading unified asset intelligence and security platform designed to address the new threat landscape that connected devices create. Our customers 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 San Francisco, California.

1.888.452.4011 | armis.com