CASE STUDY

Flavor Manufacturer Secures OT and Business Continuity Today and in the Future

Armis brings stronger security, peace of mind, and ease of management

Customer profile

Flavor Manufacturer

Industry

Food Manufacturing

IT environment

OT manufacturing and PLC equipment used by close to 100 users

Introduction

This food manufacturing business located in the northeast U.S. specializes in flavorings and other ingredients of today's rapidly evolving threat landscape, the company became increasingly concerned about ensuring business continuity, minimizing risk, and ensuring that high-value intellectual property (IP) was fully secured. Its investment in an expanding operation technology (OT) network drove a need for greater visibility and control over these devices and the network traffic they generate. The company implemented Armis to boost resiliency, visibility, and security across the company's IT and OT estate.

The company started its operations out of a single building. In the last two decades, it has gradually expanded into multiple buildings. Production employees work onsite every day, while the remaining staff work remotely or on a hybrid schedule.

The director of IT is responsible for researching and implementing new technology, building the network, finding and managing IT vendors, and supporting dayto- day IT operations. He has been with the company for many years and oversees a team of two. During his tenure, he has seen many changes in the company's technology landscape.

Exponential growth drives the need for better visibility

"The company has grown a lot. Gone are the days when I could walk around and see everything that was on the network, visit every single computer or device, and review the logs manually to see what was happening," said the director of IT. "Our technology environment was starting to expand, and we had employees scattered across our buildings. We kept adding systems and devices over the years, and it got to be too much for a small team to handle. We had very little visibility and knew we needed help to keep the environment secure."

As part of a major investment in a new production facility, the company had a third party install new programmable logic controllers (PLCs). This was a primary factor in the decision to consider Armis. "Because I had not dealt with OT before, I felt it would be helpful to have visibility into the OT network," explained the director of IT.

"What if" scenarios make a convincing argument for Armis

Maintaining business continuity and minimizing risk were also top of mind and figured into the decision to deploy Armis as part of the company's security modernization effort.

"As the director of IT, I'm constantly thinking to myself: 'What if something happens to me?' Sure, there's documentation, and I know where everything is, but how quickly would someone else be able to come in and see what's on the network?" he asked. This would be a concern for any organization, but especially for a company with a small IT team.

To his point, a ransomware incident hit when he was on vacation. The silver lining was that C-level executives were then quickly persuaded of the need to support security initiatives with more resources. "I think, previously, the feeling was, we're a small company and nobody's ever going to be interested in any of the stuff that we do. But, of course, that's not true," said the director of IT.

Challenges

- Supporting business continuity
- Safeguarding customer's intellectual property
- Gaining visibility into OT devices

Eye-opening connections highlight Armis's value in a changing security landscape and geopolitical environment

The director of IT initially learned about Armis from a local reseller, who performed a demo of the product. During the proof of value (POV), he discovered some surprising connections happening between control servers and manufacturing equipment. "The SCADA [supervisory control and data acquisition] servers were connecting to the internet, Microsoft, and Google cloud services, for example. That was quite an eye-opener," he recalled.

As a complement to Armis, he installed a Fortinet FortiGate Next-Generation Firewall (NGFW), which he considers a critical component in the company's security posture, since it is the single point through which all internet traffic flows.

"It's been very important to integrate the Fortinet firewall into Armis and get alerts if connections to the outside world occur or if there's malware dormant on the network," he asserted.

The director of IT also pointed out that, given current geopolitics, it is also critical to monitor all hardware devices, to ensure that valuable corporate data is not leaking out to foreign actors.

Armis Results

- Visibility into network traffic
- Improved IT and OT security posture
- Easy management and operationalization for threeperson IT team
- Maintaining compliance with cyber insurance requirements

Armis alerts resolve the hidden dangers of IoT devices

The director of IT called attention to the fact that the brand name on a product's packaging is not necessarily indicative of the actual manufacturer. "Let's say you install a camera, and it has some brand name on the outside of the box. Even though it has one brand name on the outside, you cannot go by the brand name, so you can't assume they are secure. You have to look at the actual traffic that these types of devices generate and then mitigate from there," he said.

Misconfiguration errors on internet of things (IoT) devices, such as certain security cameras, are a wellknown vulnerability and a potential point of entry for cybercriminals. The director of IT's solution is twofold. First, he does not allow cameras to connect to the internet. Second, he has set up alerts within Armis so that if a device does start talking to the outside world because of a configuration error, he will know immediately.

The Armis alerting systems save him and his team a great deal of time. "It's not noisy at all. The number of alerts we get are easy enough to take a look at. Recently, I got an email alert about a phishing campaign. I went to the Armis console, and I started drilling down into the assets. It was easy to make a decision as to whether it was something that needed to be addressed or not. Armis saves a lot of time in investigation," he pointed out.

"The number of alerts we get are easy enough to take a look at. Recently, I got an email alert about a phishing campaign. I went to the Armis console, and I started drilling down into the assets. It was easy to make a decision as to whether it was something that needed to be addressed or not. Armis saves a lot of time in investigation."

Director of IT
Food Manufacturer

Armis benefits: cost savings, peace of mind, and data protection

Armis's ability to automate alerts across the team and not have to constantly chase noise is a huge benefit to the small IT team.

The director of IT shared that Armis gives him more peace of mind. "I don't need to be constantly on the lookout for threats," he said. "Honestly, I haven't seen a lot of malicious activity. In the back of my mind, I keep thinking, 'Is it because it's not there or because I'm just not seeing it?' But because I have regular monthly implementation calls with the [Armis] team to solve for our use cases and discuss these types of issues, I can rest assured that the malware is not there. Armis gives me that sense of security, and I don't need to worry."

Another benefit that Armis brings is the potential for reduction in cyber insurance costs. "Recently, when I had to fill out the questionnaire for our cyber security insurance, I was able to check 'yes' for so many items I couldn't check 'yes' to before Armis," he remarked.

Perhaps most importantly, Armis helps protect the company's IP to ensure there are no leaks. The Armis platform supports the Center for Internet Security (CIS) Critical Security Controls. It flags unusual data movement on the network or from device to device and creates alerts if it sees that critical data is unencrypted.

Security and risk management now occupy a more prominent seat at the table and are becoming top priorities for both the IT team and upper management. "Five years ago, things were very different, and companies were not paying much attention to security. It's just amazing how quickly that has changed," observed the director of IT.

With an improved security posture—thanks to Armis—at its manufacturing facilities and in its IT environment, the food manufacturer is well-positioned to continue serving its customers and dessert lovers everywhere for years to come.