CASE STUDY

Armis Helps Ensure Ongoing Delivery of Critical Therapeutics to Patients

Multinational bio-pharmaceutical company minimizes supply continuity risks at manufacturing plants

Customer profile

Focuses on research and production of potentially life-changing treatments for specific medical conditions.

IT environment

Highly distributed, with approximately 52,000+ employees across 80+ worldwide locations and 45 manufacturing plants in 20 countries

Industry

Biopharmaceuticals

Introduction

Takeda Pharmaceuticals focuses on research and production of potentially life-changing treatments for specific medical conditions. The company is dedicated to the timely delivery of medicines to those who need them. By providing comprehensive visibility into laboratory and production equipment in its manufacturing plants, Armis has vastly improved the company's cyber resiliency and increased confidence in its ability to maintain supply continuity.

Takeda Pharmaceuticals, a large global life sciences enterprise spanning over 80+ countries, pursues life-changing treatments for patients across four therapeutic areas, including oncology, gastrointestinal disorders, neuroscience, and rare diseases. The company has 45 manufacturing centers in 20 countries with specialized systems for creating biologics, pill-based medicines, and other treatment types.

Over the years, Takeda has grown rapidly through acquisitions, resulting in a disjointed manufacturing network with a mix of aging and newer equipment. Given the growing prevalence of destructive cyberattacks that target intellectual property and could potentially disrupt ongoing operations within or across plants, Mike Towers, chief security and trust officer at Takeda Pharmaceuticals, was increasingly concerned about the security of plant systems and assets.

Like any manufacturing environment, Takeda's plants include industrial control systems and many specialized assets that do not work with agent-based security solutions. Any given plant could include things like refrigeration units, mass spectrometry equipment, chemical mixing machines, and more. These machines are very expensive. For example, just creating a cell therapy or a gene therapy product for an advanced cancer may cost up to 150 million dollars. Moreover, many of the devices are integral to monitoring temperature, humidity, and other environmental conditions in plants that are key to quality and are connected to the internet for maintenance and to collect data. The problem was that Towers and his team didn't have any way to see or secure large numbers assets across Takeda plants.

Speedy time to value makes Armis the top choice

To solve this security and visibility gap, Towers evaluated three vendors, including Armis. The Armis proof of value (PoV) was in Takeda's Brooklyn Park facility, outside of Minneapolis, Minnesota. Prior to the Armis PoV, Towers and his team estimated there were about 100 network-connected devices in the Brooklyn Park facility. With the help of the Armis Asset Intelligence Platform, they soon realized the plant actually included more than 980 connected devices. Based on the PoV, Takeda rolled out the Armis platform across all of its plants and within about six weeks Towers says his team identified more than 42,000 devices in the plants across the globe, 18,000 of which are critical to the manufacturing process.

"Of all the vendors we looked at, Armis provided the fastest time to value and the widest coverage. Because it's cloud-based, Armis is also simple to manage. All these factors made it easy to choose Armis, frankly," says Towers. "Thanks to Armis, we've already uncovered a series of potential cyber risks. Without the Armis deployment, we never would have known they existed. It has already paid for itself."

Takeda turned to Amazon Web services (AWS) for an initiative to empower self-service, on-demand access to cloud technologies across the organization. With this project, it aimed to migrate its business applications in core data centers to AWS and other software-as-a-service solutions and rationalize its technology estate. Takeda also leveraged the Armis connectors and collectors running on AWS to gain full visibility of the IT assets connected to their corporate network.

Resolving supply chain continuity risk

For Takeda Pharmaceuticals, one of the biggest risks is a disruption in supply chain continuity, which would slow or prevent the delivery of medicine to patients. "The most likely cause for not getting product to patients is a potential incident where a cyberattack takes a plant down and renders the computer-driven devices unusable.

We primarily deployed Armis for this use case—to improve our supply continuity and the resiliency of our overall manufacturing process," explains Towers. "At Takeda, nothing comes before making sure that we get our medicines to patients, and Armis is one of the key contributors to making sure that we can do that."

Challenges

- Limited visibility into connected assets across an extensive network of manufacturing plants
- Difficulty understanding and managing supply continuity risks
- Prevention of potential outages and downtime at manufacturing facilities
- Lack of security controls to protect against emerging threats targeting intellectual property and production and lab equipment

Since deploying Amis, two global plants in the organization's biggest therapeutic areas have seen vastly improved supply continuity. One plant focuses on oncology creating medicines to help treat advanced types of cancer. Another plant makes a powerful biologic that treats colitis, Crohn's disease, and rheumatoid arthritis.

"These are just two examples. Armis allows us to have a lot more predictability and quality assurance for all the products that come out of those two plants," notes Towers. "Because Armis provides passive, always-on monitoring, we have reduced unplanned downtime related to system issues or cybersecurity events."

Armis strengthens Takeda's compliance program

In the highly regulated pharmaceutical industry, the ability to demonstrate proper security controls in manufacturing labs is integral to regulatory compliance. And for a large, globally distributed company like Takeda, it can also be incredibly challenging and time consuming.

To streamline compliance-related processes at Takeda, Towers and his team launched an internal initiative that they call Manufacturing Lab Security (MLS).

"One of the primary reasons for the MLS program is to improve the quality and the regulatory compliance of our manufacturing process and to demonstrate due care in protecting these environments from outages and from any risks to resiliency or availability. We were able to use Armis to help us with compliance submissions and to show demonstration of control," affirms Towers.

Armis integrations lead to better insights and improved hygiene

To get the most from the Armis platform, Towers and his team prioritized several integrations, including an integration with its Splunk environment. The team also integrated Armis with its Exabeam analytics engine, which focuses on user and entity behavior analytics to discover risky behavior by people and devices on the network. Armis consolidates, cleans, and enriches data to provide a single, authoritative view of asset truth behind

"Of all the vendors we looked at, Armis provided the fastest time to value and the widest coverage. Because it's cloud-based, Armis is also simple to manage. All these factors made it easy to choose Armis, frankly," says Towers. "Thanks to Armis, we've already uncovered a series of potential cyber risks. Without the Armis deployment, we never would have known they existed. It has already paid for itself."

Mike Towers
Chief Security and Trust Officer
Takeda Pharmaceuticals

a single pane of glass so Towers' team can better understand and respond more rapidly to potential threats.

Armis is also helping with the team's workflows. To optimize the accuracy of asset data in the configuration management database (CMDB), Towers and his team integrated Armis with ServiceNow. And an integration with Tanium provides Towers and his team assurance about the security hygiene of the organization's digital infrastructure and assets and helps simplify compliance.

One platform, a host of benefits

Takeda has benefited from the Armis deployment in several ways. But according to Towers, the top benefit is unprecedented and complete visibility into all devices in the manufacturing plants. The team loves having a single-pane-of-glass management platform with all asset information consolidated into easy-to-access, user friendly dashboards.

"We have more centralized and consistent control in an environment that had no standardization whatsoever prior to Armis. Now we have a single asset repository and a single asset management solution for our entire manufacturing network, which before was duplicated 50 times," says Towers. "We've been so successful in the plant environment that we will be implementing Armis on the enterprise side as well."

Towers also notes that continuous, real-time asset monitoring is a key benefit. Now his team can easily explore the current inventory and the state of their devices with respect to configurations and security updates. They are also alerted to changes in network patterns, enabling faster responses to potential threats. "Armis constantly provides us up-to-date information. Any deviation from normalcy in these environments is very, very important to look at from a security perspective," remarks Towers.

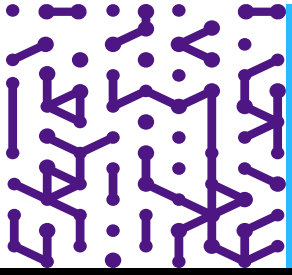
Looking ahead

Towers and his teams are already forging ahead with expanding the use of Armis in Takeda. Next up, the team plans to implement the Armis Asset Vulnerability Management module to get more control over the cyber risk management lifecycle. They will also extend Armis to the organization's 200 blood plasma donation centers, which Towers describes as "highly variable environments." He says that it's critical to secure these centers because plasma is a key ingredient in many of the medicines developed by Takeda.

Armis Results

- 100% visibility into connected assets in the manufacturing environment
- Increased assurance of uptime and supply continuity
- Consolidated, easy-to access asset information in a cloud-based dashboard
- Continuous real-time monitoring of assets to determine update and configuration status and anomalous network behavior

For other biopharmaceuticals with environments similar to Takeda's, Towers recommends prioritizing the manufacturing and supply continuity challenge. "In the biopharmaceutical sector, this may seem daunting because, by design, plants have to be built differently because they do different things. But before you can do anything from a security perspective, you have to know what's in your environment. You can't protect what you don't know about. And that's where Armis comes in. It's a foundational platform that addresses that risk area, and you can extend that to other parts of the environment where there are similar challenges," explains Towers.



ARMIS.

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