CASE STUDY

Continuous Critical Therapeutics through Network Detection & Remediation

The Challenge

- Limited visibility into AWS and manufacturing plants' network activity
- Rapid growth created disparate, hybrid environments
- Lack of visibility exposed Intellectual Property & production equipment

The Solution

- 100% visibility across AWS and physical environments including accurate CMDB
- Integrate AWS native security tools data with compliance tools
- Always-on, passive monitoring with realtime remediation

The Results

- Identified 42,000 devices globally, many previously unmanaged
- "Vastly improved supply continuity"
- Reduction of unplanned downtime related to cybersecurity events

Industry Pharmaceutical manufacturing

Location Tokyo, Japan

Size 50,000 employees; $20B+ annual revenue

Background

Takeda Pharmaceuticals is a multinational pharmaceutical company headquartered in Tokyo, Japan. One of the largest pharmaceutical companies in the world, they focus on innovation, research, & development of new drugs to treat diseases & conditions in oncology, gastroenterology, neuroscience, rare diseases, and vaccines.

Limited visibility into their manufacturing network and lack of correlation with AWS assets, Taceda faced potential outages & downtime. The plant systems were not suited for agent based security and a comprehensive view into threats and traffic was required to meet internal security controls.

At the same time, Takeda was leveraging AWS Project Fulji to empower self service, ondemand access to cloud technologies across its entire organization with a goal to migrate 80% of business applications to AWS.

The Challenge

Fast growth and acquisition had created many unique manufacturing environments and private data centers. This led to significant inefficiencies and eliminating their ability to effectively manage risk. This combined with the need to prevent potential outages & downtime created significant pressure on the CIO, CISO, and both their IT & OT teams.

Takeda plants include specialized assets essential to manufacturing and unable to be modified including adding agents. Lack of visibility into these assets exposed Takeda to emerging threats targeting their intellectual property and production equipment. Additionally, no effective detection and remediation

"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."

Mike Towers
Takeda Chief Security & Trust Officer

was possible between the quickly growing AWS environments and the manufacturing floors. Mike Towers, Chief Security & Trust Officer, recognized the growing risks associated with destructive cyberattacks and sought a solution to secure plant systems and assets while streamlining their complex operational landscape with AWS & Project Fuji.

The Solution

Armis Centrix on AWS provided a comprehensive solution to address Takeda's challenges through 100% visibility across each manufacturing environment. The SaaS solution aggregates and deduplicates log & alert data from AWS CloudTrail, GuardDuty, and soon Security Hub with manufacturing specific security tools in a secure and scalable single pane of glass. The AWS based Armis Centrix platform allowed Takeda to understand the true attack surface of their plants such as their plant in Brooklyn Park where an estimated 100 OT devices proved to be over 980 unmanaged, production devices.

The Results

With the new found, auditable information on what every device is doing in all their networks, manufacturing, on-premise, and in AWS, Takeda was confident in their CMDB and internal service management tools to provide relevant & actionable remediation guidance. This new proactive risk management approach helped Takeda strengthen their supply chain's integrity, protecting their commitment to delivering life-saving medicines to patients.

Most notably, the Armis Centrix on AWS deployment led to "...unprecedented and complete visibility into all devices in the manufacturing plants." Mike Towers, Chief Security 7 Trust Officer. As a result Takeda identified more than 42,000 devices across the globe, 18,000 of which are critical to the manufacturing process.

Since implementing Armis, two global plants in the organization's biggest therapeutic areas have seen vastly improved supply continuity. One plant focuses on oncology, creating medicine to help treat advanced types of cancer, while the other makes a biologic that treats Crohn's disease & rheumatoid arthritis. Towers notes Armis on AWs allowed Takeda to have "a lot more predictability & quality assurance for all the products that come out of those two plants."

The continuous real-time asset monitoring provided by Armis has allowed Takeda to detect & respond to deviations from normalcy in their AWS and Manufacturing environments more quickly.

© Copyright Armis 2024