Case Study

# Unified View of IT, IoT, and OT Assets Aids Security and Compliance for a Major European Port

## The Challenge

- Maintaining an accurate and up-to-date inventory of all assets
- Identifying unused and end-of-life assets in the digital estate
- Complying with increasing European Union (EU) cybersecurity regulations
- Receiving alerts on all security and configuration issues resulting in alert fatigue

## The Solution

- Deployed multiple Armis Centrix™ platform products
- Provided complete and continuous asset management across the entire estate
- Identified all digital assets, including IoT and OT devices
- Used by multiple teams in the organization, including non-technical staff

## The Results

- Detected unwanted devices on the network
- Uncovered usage and device data for costly contracts and software licenses
- Surfaced end-of-life builds within the digital estate
- Uncovered laptops that lack endpoint protection

Industry: Logistics

Location: Antwerp, Belgium

Size: 1,800

- Armis Centrix™ for Asset Management and Security
- Armis Centrix™ for VIPR Pro - Prioritization and Remediation
- Armis Centrix™ for OT/IoT Security

## Background

The Port of Antwerp Bruges sits at the mouth of the Scheldt River in the Flanders region of Belgium. As the second busiest and largest port in Europe and Belgium's primary economic driver, it is a crucial hub in the continent's supply chain and global trade. It boasts the largest port locks in the world and is the fourteenth most active port in the world. With more than two decades of experience in the industry, CISO Yannick Herrebaut has helped the port pioneer new technologies and develop a reputation for sustainability and innovation, supporting a secure, redundant digital infrastructure that enables the port to operate 24/7/365.

## The Challenge

As a critical infrastructure organization, the port's primary motivation for seeking a new solution was regulatory compliance with the NIS 1 directive, which constituted the first cybersecurity legislation the port authority had to follow. In selecting a framework to guide their efforts, they chose the well-known CIS Controls, where the first two controls pertain specifically to hardware asset management and software asset management. The port

> "Before Armis, it was quite a nightmare because data was everywhere and nowhere at the same time. Where do you begin? You always have the feeling that you're protecting the things that you know about and potentially ignoring the things you don't know about. Now we really know what is happening within our environment."
>
> **Yannick Herrebaut,**
> **CISO, Port of Antwerp Bruges**

quickly realized that while they had various systems containing parts of their asset information, they lacked a holistic view of everything within their vast and dynamic environment.

The digital estate is complex, encompassing a broad spectrum of IT, IoT, and OT assets. This includes classic laptops and smartphones, specialized PCs controlling video walls, terminal-like appliances, and devices in two owned data centers (containing servers and switches) within the IT domain. The environment also includes IoT devices such as drones equipped with thermal cameras and sensors measuring air quality. Crucially, the port manages Operational Technology (OT) assets related to critical functions such as bridge and lock control, as well as HVAC systems, building automation systems for lighting, and radar systems.

Although the port used a Configuration Management Database (CMDB), it was challenging to keep the data accurate and current. "CMDBs are not the holy grail, and the data they contain does not always accurately represent the reality of your digital assets. The assets you don't know about oftentimes are the greatest risks to your organization," Herrebaut pointed out. Moreover, asset data was scattered across many siloed tools, including the ERP system, Microsoft Azure, network servers, the Network Access Control (NAC) system, and the vulnerability scanner. Therefore, the organization needed a unified asset management solution that provided a continuously updated database of all hardware and software (managed and unmanaged). The solution also needed the ability to alert the team to all security and configuration issues, such as critical vulnerabilities. A key technical requirement was compatibility with the existing technology stack via out-of-the-box API connectors to avoid the maintenance issues associated with custom integrations.

## The Solution

After evaluating multiple options, the Port of Antwerp Bruges determined that Armis Centrix™ for Asset Management and Security and Armis Centrix™ for OT/IoT Security met their requirements and agreed to a Proof Of Concept (POC).

Armis Centrix™ provided a solution by identifying all IT, IoT, and OT assets and delivering a single-pane-of-glass overview of the entire digital estate. Its holistic approach and use of passive monitoring made it uniquely suited for deployment in the OT environment. The port later expanded its license to include Armis Centrix™ for Vulnerability Prioritization and Remediation to manage vulnerabilities in both the IT and OT domains. Herrebaut was particularly impressed by the responsiveness of the Armis team during the POC phase, noting that approximately 80% of a long list of issues were resolved before the POC concluded and the contract was signed. This proactive support instilled faith in Armis's commitment.

## The Results

The implementation of Armis Centrix™ has enabled the Port of Antwerp Bruges to increase its cybersecurity maturity and generate clear value across multiple departments, extending beyond core security functions.

Armis provided immediate value by detecting previously unknown security risks. For instance, it detected unsanctioned 4G routers that contractors had installed outside of corporate channels. These routers, often used for easier remote access, posed a weak link that hackers could exploit, but Armis easily

**Decrease in time spent managing vulnerabilities**

**Increase in cost savings when managing software licenses**

**30**

**laptops found missing an EDR agent**

identified them and zeroed in on their exact physical locations. The platform also uncovered 30 laptops that lacked an active Endpoint Detection and Response (EDR) agent installed, allowing the team to mitigate this significant security risk quickly. Furthermore, Armis surfaced end-of-life builds, including those running Windows 10, helping the team plan ahead for replacements before support expires. This capability also helps identify and manage out-of-date operating systems on servers and devices—a common challenge, especially in the OT domain where legacy systems like radar units are tightly integrated and difficult to upgrade.

Armis's value extends beyond core security functions. The IT office and governance department use Armis to track granular data on expensive software and licenses, such as Microsoft Visio and Microsoft Project. This allows them to verify which devices have these licenses installed and reclaim them if they are unused, resulting in significant cost savings. Additionally, Armis assists the services team by matching their asset database in the ERP tool with what is actually deployed in the field. When manual errors occur (e.g., forgetting to register a laptop handed to a new employee), Armis can quickly track down the device by its identification code, user, or even its physical location, preventing the loss of valuable assets and correcting erroneous information in the ERP system.

The port is actively using Armis Centrix™ for VIPR Pro - Prioritization and Remediation to develop metrics and KPIs to objectively demonstrate progress to management and auditors. They track the number of critical vulnerabilities that are open across three categories: less than 7 days, less than 30 days, and less than 90 days. For the future, the port plans to continue developing advanced trend lines for these KPIs. [OO1]

Herrebaut concluded: "Before Armis, it was quite a nightmare because data was everywhere and nowhere at the same time. Where do you begin? You always have the feeling that you're protecting the things that you know about and potentially ignoring the things you don't know about. Now we really know what is happening within our environment.". He added that Armis is truly an enabler for him as a CISO, helping to increase the cybersecurity maturity of the organization and secure assets for stakeholders in various IT departments.