

## CASE STUDY

# Securing Critical OT Infrastructure for a Pharmaceutical Leader



### The Challenge

- | Lack of OT visibility
- | Manual & fragmented remediation processes
- | No prioritization framework
- | Resource limitations

### The Solution

- | Full inventory of all assets with deep situational awareness
- | Detecting security gaps, vulnerabilities and misconfigurations
- | Practical mitigation guidance and workflow
- | AI based remediation assignments

### The Results

- | 60% Security Controls Improvement
- | Comprehensive and precise asset inventory
- | Reduction in patching and remediation backlog
- | Up to 75% Resource Savings on Technical Assessment

Industry: **Pharmaceutical**

Location: **Munich, Germany**

Size: **1,000 employees**



**Armis Centrix™ for OT/IoT Security (On-prem)**

## Background

Hermes Arzneimittel Holding, a European pharmaceutical company with over 100 years of expertise, faced critical OT cybersecurity challenges. As a leader in non-prescription medicines and dietary supplements, their operations rely on highly regulated logistics and manufacturing processes. Ensuring compliance, operational continuity, and safeguarding public health were their top priorities. Armis Centrix™ for OT/IoT Security (On-prem) was deployed to resolve their primary challenges: incomplete OT asset visibility and a lack of insights, prioritization and remediation plan, which had left security gaps unaddressed and operational threats heightened. By prioritizing critical risks and delivering practical guidance, Armis Centrix™ provided a proactive approach to managing this sensitive OT environment, and directly improved operational efficiency and resilience.



*"At Hermes, we deployed the Armis Centrix™ for OT/IoT Security (On-prem) platform across all of our sites, gaining complete visibility into our OT network assets and vulnerabilities with outstanding accuracy. The platform's flexibility, combined with its unique OT-specific expertise, provides exactly the value we were seeking."*

**Kilian Helfert,**  
IT Security Officer

## The Challenge

Hermes Arzneimittel Holding faced several related issues:

1. Manual, fragmented processes: Asset management relied on quickly outdated spreadsheets and manual processes, prone to data loss and errors, making the OT environment difficult to secure and operate.
2. Lack of OT visibility: Blind spots left vulnerabilities unidentified and unmitigated, exposing the organization to compliance gaps and operational risk.
3. No prioritization framework: The absence of full visibility and operational context made it difficult to address high- impact issues efficiently.
4. Resource limitations: Limited on-site OT security personnel and reliance on remote IT expertise slowed mitigation efforts.

A prior IT-focused solution deployment failed to deliver deep, meaningful assets, attributes and context, emphasizing the need for an OT-specific approach.

## The Solution

Armis Centrix™ for OT/IoT Security (On-prem) addressed these challenges by providing full asset visibility and streamlined IT and OT workflows, while setting a robust foundation for future security program expansion:

- **Extensive data collection and comprehensive asset visibility:** Armis Centrix™ for OT/IoT Security (On-prem) provided an accurate, context-rich asset inventory, mapping all IT, OT and IoT assets- including legacy equipment- down to level 0 I/O devices. It combined cross-channel data collection through robust third-party integrations, industrial integrations, passive network monitoring, and Safe Active Query, enriched with AI-driven insights to deliver high-fidelity attribution and insights that grow as integration deepens. Armis Centrix™ for OT/IoT Security (On-prem) mapped all assets, including their roles and interdependencies, offering valuable intelligence into their potential operational impact.
- **Prioritization at the core:** Armis Centrix™ for OT/IoT Security (On-prem) asset-centric approach filtered noise and reduced the number of alerts, while also prioritizing high-risk events that required immediate action.
- **Exposure Management:** Included detecting security gaps and misconfigurations, identifying end-of-life assets, security controls validation effectiveness by analyzing the coverage and utilization of firewall configurations and EDRs, assessing the attack surface and identifying attack paths to critical assets.
- **Quick deployment:** Quick onboarding, light training module and an intuitive, customer- centric interface allowed both IT and operational teams to utilize the platform upon deployment.
- **Practical mitigation guidance:** The platform automatically assessed operational units risk levels and provided step-by-step recommendations and playbooks, bridging skill gaps and enabling operational teams and security practitioners to prioritize critical vulnerabilities and address them efficiently.



60%

Security Controls  
Improvement

Presenting precise  
inventory based on Safe  
Active Query shortly Upon  
Deployment

Up to

75%

Resource Savings on  
Technical Assessment

## The Results

**Shortest time to value:** Armis Centrix™ for OT/IoT Security (On-prem) delivered comprehensive OT asset visibility. Previously undocumented devices were identified, creating a robust and reliable asset inventory while leveraging existing security stack.

**Trust in Safe Active Query technology:** The Safe Active Query mechanism earned the customer's trust by safely enabling ultra-rich data collection. This gradual process, tailored for OT environments, proved both effective and secure within their sensitive production setting. Granting access in such a critical environment was a clear testament to the reliability of Armis Centrix™ for OT/IoT Security (On-prem) technology.

**Bridging skill gaps:** The platform's step-by-step mitigation playbooks empowered teams to immediately implement remediation steps, driving effective risk reduction.

**Accurate vulnerability mapping:** By deduplicating, correlating, and contextualizing vulnerabilities with specific assets and operational processes, the platform eliminated false positives, enabling optimal resource utilization and a cost-effective course of action.

**Compliance integration:** With built-in compliance measures, Armis Centrix™ for OT/IoT Security (On-prem) automated IEC 62443 readiness, reducing the customer's regulatory burden.

**Exceeding expectations:** Deploying Armis Centrix™ for OT/IoT Security (On-prem) has met and exceeded the customer expectations, providing a streamlined, stable OT stance, reducing MTTD and MTTR.

**Evolving security needs:** Establishing a solid foundation that provides a unified, scalable and , centralized view across all sites and assets, as the organization's security needs evolve.



1.888.452.4011  
www.armis.com

**Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.**

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. 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 stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

