SOLUTION BRIEF

Secure and On-time Delivery for Transportation and Logistics Infrastructure with Armis

Introduction

> From moving people via cars, trains, planes, and boats to shipping goods across various terrains and through multiple modalities such as road, rail, sea, and air, the transportation encompass a broad range of sub industries. This sector can also be described as critical infrastructure and relies on Operational Technology (OT) to maintain the integrity and reliability of the intricate systems on which global economies depend. An interruption, even briefly, due to a security breach, can lead to a potentially catastrophic fallout.

The Transportation and Logistics Landscape

The World Economic Forum suggests that digitalization could unlock approximately $1.5 trillion in business opportunities for transportation and logistics players by 2025. With this in mind, the pressure is on for organizational leaders to take the leap and invest in the future of cybersecurity. Digital transformation has made the supply chain more efficient and circular, leveraging existing technologies at lower costs, optimizing raw materials, and enhancing transport management.

Recent advancements include automated warehousing, high-speed rail, last-mile optimization, and software-based innovations such as intelligent transportation systems, predictive maintenance, drone supervision, and of course artificial intelligence.

Consequently, the transportation and logistics industry now generates vast amounts of structured and unstructured data. Advanced technologies like AI are essential for strategically managing this data. By mapping information from connected equipment and logistics software to machine learning models in the cloud and comparing that data to industry standards, businesses can achieve greater supply chain transparency and significantly reduce operational expenses.

OT Examples in Transportation:

At airports, Operational Technology (OT) plays a pivotal role in streamlining processes such as baggage screening, fuel coordination, maintenance scheduling, aircraft servicing, and plane provisioning.

Within the maritime shipping sector, OT is integral for orchestrating shipping timetables, ship loading operations, and the real-time monitoring of vessels and individual cargo containers.

On the roadways and railways, OT systems enhance efficiency through the management of traffic signals, road conditions, route planning, and maintenance tasks, among other functions.

For public transportation networks, OT technologies are vital for the precise management of schedules, passenger information, fare collection systems, and vehicle tracking, thereby ensuring the delivery of reliable services.

In the automotive sphere, OT contributes significantly to vehicle diagnostics and function management, the advancement of safety features, and the improvement of fuel efficiency, all in aid of superior environmental outcomes.

Within the logistics and warehousing industry, OT applications are key to automating inventory control, refining order processing, and optimizing the logistical flow of goods into and out of storage facilities.

Regarding cycling and pedestrian pathways, OT solutions enhance both safety and accessibility through the monitoring and management of lighting, signals, and pathway conditions in real time.

Real World Attacks on the Transportation and Logistics Sector

April 2021

MTA

Attack on the New York City Metropolitan Transportation Authority. The breach was the third cyberattack on the transit network, North America's largest, by hackers thought to be connected to foreign governments in recent years, according to transit officials.

August 2023

KNP

UK-based KNP Logistics group shut down permanently by major ransomware attack that impacted key systems, processes and financial information.

November 2023

Boeing

Days after a Russian-affiliated ransomware group claimed responsibility for a cyber breach, Boeing confirmed a cyberattack was affecting Global Services operations.

September 2023

ORBCOMM

Trucking and fleet management company ORBCOMM experienced a ransomware attack that is temporarily impacting our FleetManager platform and BT product line, which is used by some of their customers to track and monitor their transportation assets.

Why Are Transportation and Logistics Environments Being Targeted More Year on Year?

01 Increased Digitization and the Convergence of IT/OT

The transportation and logistics industry has undergone significant digitization in recent years. While this transformation has improved efficiency and connectivity, it has also expanded the attack surface for cybercriminals. Integrated IT and OT environments mean that compromising one system can often grant access to others, making these sectors attractive targets.

02 Assets on the Move

Highly distributed assets are difficult to keep secure especially when they are constantly in motion. As a result, they are more easily susceptible to cyber exposure and attack.

03 High Impact and Visibility

Attacks on critical infrastructure and OT systems in transportation and logistics can cause widespread disruption, making them lucrative targets for cybercriminals seeking high-impact outcomes. The ability to halt operations, delay shipments, and cause public panic increases the likelihood of ransom payments and media attention, which can be appealing to attackers.

04 Economic Incentives

The transportation and logistics industry is vital to the global economy. Any disruption can have cascading effects on supply chains, leading to significant financial losses. Cybercriminals leverage this vulnerability to demand higher ransoms, knowing that companies might be more willing to pay to resume normal operations quickly.

05 Vulnerability of Legacy Systems

Many transportation and logistics companies still rely on legacy OT systems that were not designed with cybersecurity in mind. These outdated systems often lack modern security features, making them easier to exploit. Coupled with the challenge of securing complex, interconnected networks, this makes OT systems particularly vulnerable.

06 Geopolitical Motivations

State-sponsored cyber attacks have become more prevalent as part of geopolitical strategies. Critical infrastructure, including transportation and logistics, is a prime target for nation-states looking to disrupt the economic stability of adversaries. Such attacks can serve as a form of economic warfare, creating long-term strategic advantages.

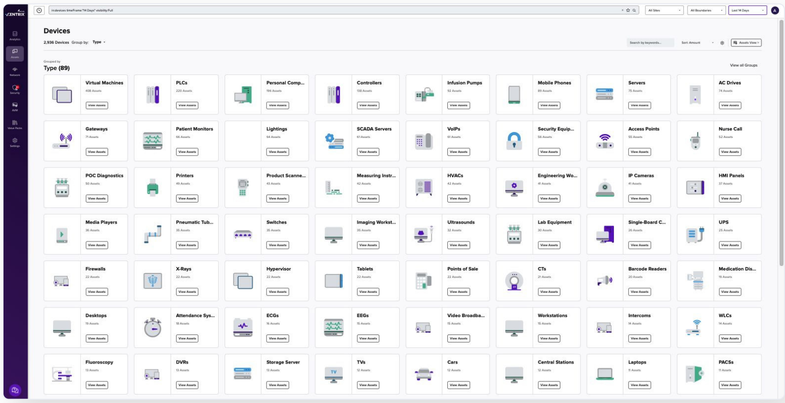
Armis Centrix™ Secures the Entire Lifecycle of Your Transportation Assets

As modern transportation and supply chain networks become increasingly complex, the need for seamless integration and coordination between diverse systems is paramount. This complexity requires infrastructure that is not only intelligent but capable of real-time tracking and coordination of a broad range of assets. To achieve real-time operational capabilities and adapt to changes swiftly, these systems must be interconnected, both among themselves and with the internet.

In this context, ensuring the visibility, security, and control of your OT infrastructure is no longer optional; it is vital for reliable and efficient operations. Armis understands the unique challenges faced by the transportation sector. The platform offers products that can offer an entire end-to-end service, from proactive mitigation with Actionable Threat Intelligence to Vulnerability Prioritization designed specifically for OT environments. With Armis Centrix™ for OT, transportation entities can proactively protect against threats and minimize disruptions.

Complete Visibility Across Complex Estates

In transportation environments, there are many systems that must work in perfect synchronization with each other for successful operations. For example, in an airport, a plane that just landed often has less than a 90-minute turnaround. To ensure a safe and on-time departure, teams and systems must work together to successfully assign a gate and execute unloading, re-provisioning, maintenance, fuel, flight routes, weather, aircraft weight, and physical security protocols and other critical operations. The systems that make all of this happen rely on a converged IT/OT infrastructure.



in:devices timeFrame:"14 Days" visibility:Full

Devices

2,936 Devices Group by: Type

Grouped by

Type (89)

Virtual Machines 408 Assets	PLCs 220 Assets	Personal Comp... 196 Assets	Controllers 138 Assets	Infusion Pumps 92 Assets	Mobile Phones 89 Assets	Servers 75 Assets	AC Drives 74 Assets
Gateways 71 Assets	Patient Monitors 66 Assets	Lightings 64 Assets	SCADA Servers 61 Assets	VoIPs 61 Assets	Security Equip... 56 Assets	Access Points 55 Assets	Nurse Call 52 Assets
POC Diagnostics 50 Assets	Printers 49 Assets	Product Scanne... 43 Assets	Measuring Instr... 42 Assets	HVACs 42 Assets	Engineering Wo... 41 Assets	IP Cameras 41 Assets	HMI Panels 37 Assets
Media Players 36 Assets	Pneumatic Tub... 35 Assets	Switches 35 Assets	Imaging Workst... 35 Assets	Ultrasounds 32 Assets	Lab Equipment 30 Assets	Single-Board C... 26 Assets	UPS 25 Assets
Firewalls 22 Assets	X-Rays 22 Assets	Hypervisor 22 Assets	Tablets 22 Assets	Points of Sale 22 Assets	CTs 21 Assets	Barcode Readers 20 Assets	Medication Dis... 19 Assets
Desktops 19 Assets	Attendance Sys... 18 Assets	ECGs 16 Assets	EEGs 15 Assets	Video Broadba... 15 Assets	Workstations 15 Assets	Intercoms 14 Assets	WLCs 14 Assets
Fluoroscopy 13 Assets	DVRs 13 Assets	Storage Server 13 Assets	TVs 12 Assets	Cars 12 Assets	Central Stations 12 Assets	Laptops 11 Assets	PACSs 11 Assets

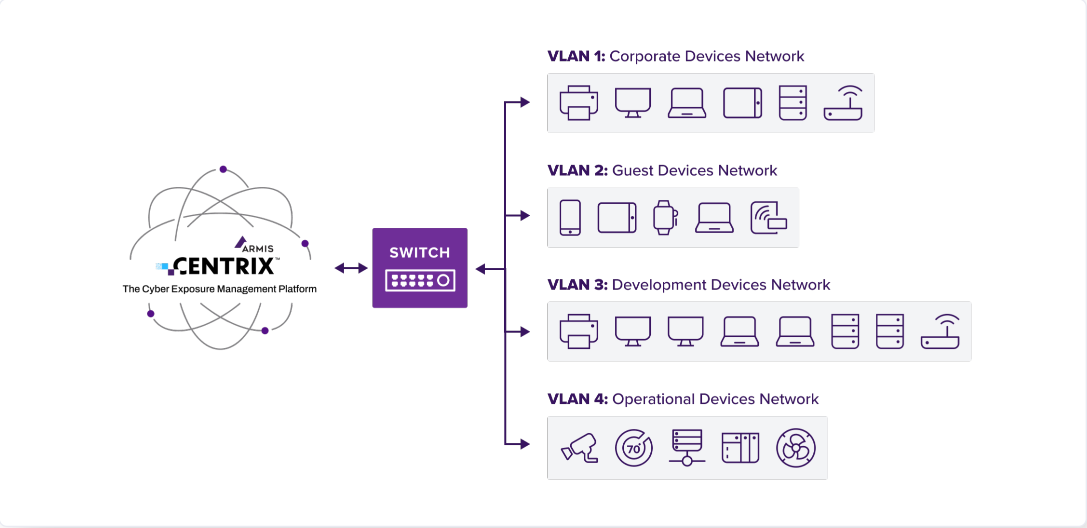
As such, complete 360-degree visibility across the entire infrastructure will ensure there are no security blind spots that can potentially disrupt or disable operations. Visibility must be at the network level to identify questionable or anomalous traffic, and at the device level to find infected devices that may or may not communicate on the network. Further, since attacks can form in one area and quickly proliferate to another, visibility should include both IT and OT devices.

Proactive Threat Management

Leveraging AI technologies for proactive threat detection, Armis employs sophisticated algorithms and machine learning with its Asset Intelligence Engine to identify and respond to cybersecurity threats in real-time. This advanced capability enables the preemptive recognition and mitigation of sophisticated cyberattacks that traditional security tools might miss.

Armis Centrix™ for Actionable Threat Intelligence is revolutionizing how Transportation organizations proactively understand and mitigate risk. In an era where transportation and logistics sectors face heightened threats from attackers, Armis provides a comprehensive view of industry events, allowing organizations to stay ahead of potential risks. Armis's insights into potential threats targeting transportation and logistics organizations is empowering them to understand their impact and take preemptive action. With human intelligence, smart honeypots and state of the art research, Armis Centrix™ ensures timeliness, unparalleled coverage and accuracy, enabling organizations to stay ahead of evolving cyber threats and protect their critical assets with confidence.

Network Segmentation and Policy Enforcement


ARMIS
CENTRIX™
The Cyber Exposure Management Platform
SWITCH
VLAN 1: Corporate Devices Network
VLAN 2: Guest Devices Network
VLAN 3: Development Devices Network
VLAN 4: Operational Devices Network
70

Armis helps transportation organizations create and enforce network segmentation policies that protect critical systems. By providing comprehensive visibility into connected assets and their communications, Armis can segment or recommend network segmentation policies that are automatically enforced via existing firewalls and network access control (NAC) solutions. This ensures critical systems are isolated from potential threats, enhancing overall cybersecurity resilience.

Manage Dispersed OT Assets Proactively to Minimize the Attack Surface Continuously

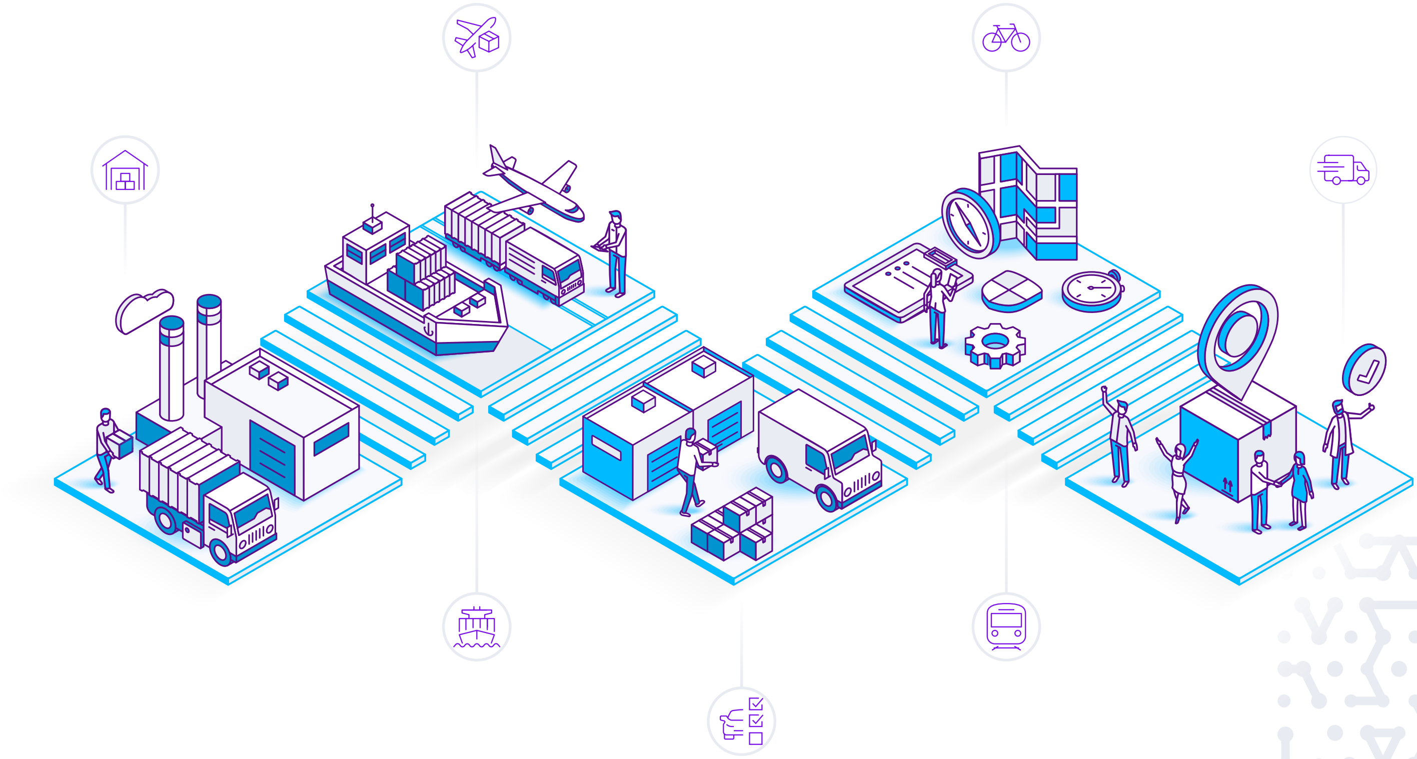
Governance requires an array of options for swift mitigation or remediation, as well as knowing which option to use based on all available intelligence. Basic options include automating workflows to open a ticket or notify an OT engineer to check a misconfiguration. More stringent options include automated remediation, network access control, dynamic segmentation, and cross-product orchestration. Patching is typically the first form of remediation when a vulnerability is discovered. But patching OT devices is notoriously difficult, due to their mission-critical nature. Systems need to be stopped and restarted to load patches, which means downtime, and some processes and equipment need to be shut down slowly for safety reasons. Instead of patching, vulnerable devices must often be segmented from other parts of the network and monitored to detect any unwanted changes in behavior.

Armis automates response workflows, including SIEM/SOC incident response and dynamic segmentation, to protect high-risk networks and keep mission-critical assets online. By connecting to your existing security ecosystem, Armis is able to bring together your ticketing systems like Jira to improve the efficiency of your stack.

Addressing Vulnerabilities and Other Security Findings Effectively

Transportation and Logistics Organizations are faced with a deluge of security alerts, with no scalable and automated way to prioritize them and operationalize remediation. This results in long lag times between the “finding”, assigning of the “owner” and the “fix”. Armis Centrix™ goes beyond vulnerability management to find and consolidate security findings across all sources to holistically understand risk and automate prioritization. Armis Centrix™ streamlines the entire remediation lifecycle, from identifying owners to operationalizing fixes, providing a unified platform for prioritization and efficient risk resolution management.

Transportation Environments are Complex, Armis has it Covered



Conclusion

Operational Technology (OT) cybersecurity is now recognized as a critical component in ensuring a reliable, efficient, and safe transportation environment. To mitigate associated risks, full visibility, security, and control over operational assets are imperative. Armis delivers comprehensive visibility across both IT and OT assets. Our asset inventory precisely identifies every asset within your environment, offering deep situational analysis down to the firmware and backplane level.

Proactive threat hunting strategies identify weak points before potential threat actors can exploit them. Vulnerability management prioritizes vulnerabilities with known exploits that are pertinent to your specific environment. Network controls meticulously tracks and documents any changes made to your OT infrastructure, enabling auditing and rollback when necessary. Armis's flexible deployment options and integration with leading IT security vendors ensure that transportation infrastructures operate with enhanced safety and reduced risk.

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