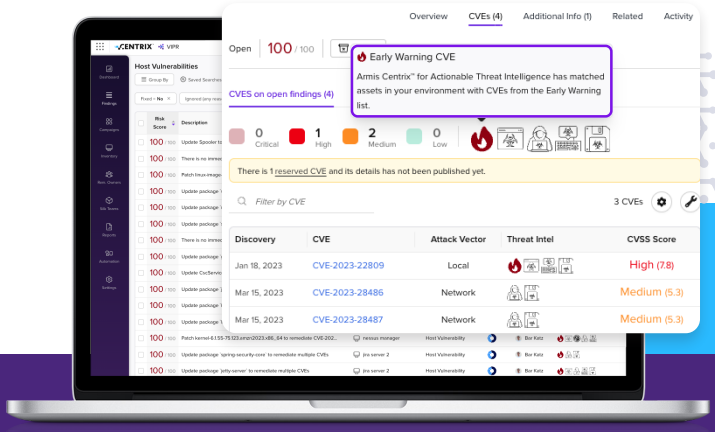
Securing Airports with Armis Centrix™

See, Protect, and Manage all Assets

The rapid evolution of the airport cybersecurity landscape has introduced significant challenges for both large and small airports. These complex environments must secure landside and airside operations against various cyber threats. The proliferation of connected assets and the integration of advanced technologies in airport operations have made maintaining robust cybersecurity measures more critical than ever.

Stringent security measures are essential to preventing major threats like terrorism and relatable inconveniences, such as canceled flights. Major threats, such as cyberattacks that target airport systems, are significant and can lead to severe consequences. However, relatable inconveniences like longer wait times and delays are more common, disrupting travel plans, grounding flights, and causing financial losses for airports and airlines. These issues can severely impact an airport's brand and reputation, making it imperative to address cybersecurity vulnerabilities proactively.

2 in 5	2 in 5 transportation and logistics assets remain unmonitored and pose the biggest threat to organizations globally - **Armis Lab**
55%	At least 55% of transport and logistic employees feel they are ill-equipped to identify or handle a significant cyberattack - **Positive Technology**
36%	36% YoY increase in the number of successful attacks on the global transportation industry - **IBM**



Why Armis is the Go-To Platform for Total Exposure Management

Complete, Real-time Visibility into the Entire Estate

From shared systems (Baggage Handling Systems, Check-in, Passenger Boarding Bridges), shared networks (Airport, Airline, and Tenants), flight information displays (FIDS), and improvement projects (Terminal Enhancements, Contractor BYOD), Armis Centrix™ goes beyond basic asset discovery. It involves collecting extensive and accurate information about each asset, including its characteristics, configurations, behavior, relationships, and vulnerabilities, to ensure operational continuity and public safety.

Empower Network Segmentation

Armis Centrix™ enables secured network segmentation implementation by discovering all assets, communication paths, and access controls. It then builds virtual barriers that restrict unauthorized access to sensitive OT assets and mission-critical systems. By limiting the scope of potential breaches, organizations can mitigate the risks posed by cyber threats, including ransomware attacks and data breaches.

Understand and Adhere to Regulatory Requirements

As critical infrastructure, airports are required to comply with stringent regulations like TSA Security Directives and NIS2. Armis Centrix™ assists airports in implementing essential security measures through network segmentation policies and controls, access control measures, continuous monitoring and detection strategies, as well as vulnerability prioritization and remediation solutions. These measures help to reduce the risk of exploitation and unpatched systems, ensuring the protection of critical infrastructure and adherence to compliance requirements.

Bridge the IT / OT and IoT Gap

Beneath the surface, airports operate as a complex network of IT, OT, and IoT systems that ensure seamless functionality. While the threats of IT-related cyberattacks, such as data breaches and ransomware, are well-documented, it is the comparatively vulnerable OT and IoT systems that represent even greater dangers. Armis Centrix™ provides a powerful cybersecurity solution specifically designed to see, protect, manage, and optimize all OT, IoT, and ICS assets, systems, and processes in your environment. This ensures both airport operational continuity and public safety.

Address Vulnerabilities and Other Security Findings

Airports are faced with a deluge of vulnerability and security alerts, with no scalable and automated way to prioritize them and operationalize remediation. Armis Centrix™ deploys advanced threat detection systems that can monitor asset behavior as well as network traffic in real-time and identify suspicious activities. Streamline your process and achieve operational efficiency by focusing on finding risk, including early warning exploit intelligence, prioritizing response, identifying the owner, and operationalizing the remediation lifecycle.

Enable Cyber-Physical Security

Armis Centrix™ integrates cybersecurity with physical security, which is essential for safeguarding airport infrastructure. It focuses on securing access to critical areas and monitoring OT and IoT asset access. By combining threat intelligence from cybersecurity and physical security, airports can comprehensively understand potential risks.

ARMIS

Key features that make Armis the go-to platform for total exposure management

- Create a detailed inventory of and manage all assets connected to airport networks, managed and unmanaged, IT OT, IoT or ICS.
- Bridge the IT/OT gap. Air gapping is no longer a valid means of securing your environment.
- Create policies and queries that highlight boundary violations, then automate your segmentation processes with intelligent recommendations.
- Assist your zero trust architecture. This framework ensures that all assets and users are continuously verified.
- Define segments for IT/OT areas of your organization, and ensure you're communicating across segments.
- Identify any abnormal or risky activity with anomaly detection and policy-based rules.
- Monitor connectivity and track asset behavior.
- Create a real-time asset inventory.
- Monitor and audit changes of ICS assets.
- Track and report errors produced by ICS assets and misconfigured ICS assets.
- Admin-configured smart active and passive discovery to safely deep dive into asset visibility through smart querying.
- Actionable Threat Intelligence that allows you to leverage insights on what threat actors are exploiting in the wild or about to weaponize.

Why Airports **are trusting Armis to deliver better outcomes**

1. **ROI** with production agility and efficiency improves MTTR by as much as 90%.
2. **Cyber Resilience** with complete asset discovery ensures visibility of all assets connected into your organization.
3. **Future-Proofed Cybersecurity** with Armis, organizations are ready for future digitalization.
4. **Operational Resilience** to reduce ransomware attacks on their critical infrastructure.
5. **Compliance and Safety** across the entire production process in manufacturing and critical Infrastructure.
6. **Reputation and Trust.** Organizations using Armis are industry leaders that advocate best cybersecurity practices.
7. **Speed of Deployment** is critical in transportation, where quick resolution and reduction of risk is a high priority.