ARMIS BUYER'S GUIDE

Keeping Air Travelers Safe on the Move

Armis Centrix™ provides full visibility into landside and airside systems, strengthening their cybersecurity posture to protect against evolving threats and providing a path to regulatory compliance.

Introduction

Airport authorities rely on a complex system of information technology (IT), operational technology (OT) and Internet of Things (IoT) to deter hostile actors and keep airport operations running smoothly.

Terminal operations technology is particularly vulnerable to disruption. Systems are network connected and have many components that expand the attack surface — from landside reservation check-in kiosks, flight information display screens, security cameras and explosive detection systems (EDS) to airside checked bag inspection systems, checked bag resolution areas and passenger boarding bridges. In addition, traditional security software may not work on many OT and IoT devices.

Recent news headlines show how a failure in one part of the system can ripple throughout the travel process and bring airport operations to a standstill. In July 2024, a flawed CrowdStrike software update shut down passenger check-in and screening checkpoints at multiple airports and grounded flights at major airlines around the world. In September, a ransomware attack at Seattle-Tacoma International Airport caused an internet outage that disrupted reservation check-in systems, flight information display screens, baggage-sorting systems and phone service.[1]

Airport authorities need a comprehensive cybersecurity strategy to protect terminal operations, meet specialized security requirements and comply with new Transportation Security Administration (TSA) regulations. This buyer's guide covers key criteria and capabilities to keep critical airport infrastructure secure and available.

[1] https://mynorthwest.com/3987234/port-of-seattle-sea-tac-airport-outage-ransomware-attack-ransom-not-paid/

Protecting Travelers and Preventing Disruptions

Airport authorities face a range of challenges when protecting terminal operations.

01 Airport operations are complex

Airports depend on a web of interconnected IT, OT and IoT devices. Mapping this ever-expanding attack surface; properly segmenting critical assets from public networks; and detecting, prioritizing and mitigating threats are increasingly difficult tasks. Traditional agent-based security solutions and vulnerability scanning aren't feasible because they can crash OT and IoT devices.

02 Constant infrastructure upgrades and terminal enhancements introduce risk

It's hard to maintain an accurate understanding of the overall attack surface when change is constant. Third-party suppliers, shadow IT and contractors bringing their own devices or gaining unauthorized access to networks introduce vulnerabilities.

03 Outdated OT systems and infrastructure are easy targets

Legacy systems were not built with cybersecurity in mind. Depending on their age, vendors may no longer offer updates or patches to address functionality or cybersecurity issues.

04 Attacks are constant

The speed, sophistication and scale of attacks against critical infrastructure are escalating, increasing the risk of disruption. Adversaries use artificial intelligence (AI) to amplify ransomware, distributed denial of service (DDoS) and phishing attacks.

05 Staffing shortages and manually intensive processes strain security teams

These factors slow down response times and increase the likelihood of critical errors.

06 Lack of asset visibility and control increases risk

Organizations need to see, manage and protect their entire attack surface to protect OT, IoT and IT assets. "Before you can protect against risks and vulnerabilities, you need a comprehensive understanding of all the assets on your network," says Russell Yeager, strategy director for airports at Armis.

07 Organizations must meet stringent regulatory requirements

These requirements include new TSA rules related to network segmentation, monitoring and detection; patching and updates; access control; and National Defense Authorization Act (NDAA) 889 prohibitions against procuring equipment and services from Russia and China.

Strategies for Better Air Terminal Security

Consider these best practices when choosing a solution to view, manage and protect OT, IoT and IT environments.

Maintain a complete asset inventory

Visibility is critical to obtain an accurate inventory of system assets and to control the attack surface. Airports typically use a configuration management database (CMDB) to track configuration information for their IT assets. But CMDB records often lack data on OT and IoT devices and virtual and cloud-based assets.

"In many cases, their CMDB is just a list of devices from as many data sources as possible that they've compiled into a spreadsheet. It tells them how many assets they have in their environment, but it doesn't provide sufficient context to fully understand their asset inventory," says Yeager.

Security organizations often use device agents to capture information and help manage network devices. But these agents can cause malfunctions and degrade performance on IoT and OT devices. IoT and OT assets may also use protocols that conventional security tools can't detect.

Modern CMDB enrichment tools automatically push contextualized and comprehensive IT asset data into your CMDB.

Bottom line

You need an flexible, non-intrusive solution that passively and continuously tracks device type, location, manufacturer, OS version, reputation and connections.

Questions to ask

- How do you discover assets that connect to the network?
- Do you have a complete and up-to-date asset inventory across all asset types, including IoT, OT, IT and cloud?
- How much manual work is involved?
- Do you trust the data?
- Would your organization benefit from CMDB enrichment tools that automatically update your asset inventory with comprehensive information, including user, classification and location?

Promote IT hygiene and address technical debt

Timely security patches and updates are a key requirement of the TSA's recent amendments.[2]

Visibility is essential to identify devices that need updates and patching, have reached end of life or end of support, or have been installed without network administrators' knowledge.

Although traditional vulnerability scanning is an important tactic for identifying and remediating vulnerabilities, it can be detrimental in an OT environment. OT devices can't withstand the traffic generated by typical vulnerability scanners. Scanning can crash the device and cause physical damage.

Bottom line

If you don't have a continuous, passive, flexible and non-intrusive solution, you won't be able to maintain good IT and security hygiene on devices that can't tolerate a software agent or vulnerability scanning.

Questions to ask

- How do you keep track of assets that need to be upgraded or patched?
- Do you have systems that should have been retired?
- Are you sure they have been disconnected?
- Are you paying for too many/not enough licenses?
- How do you track expired licenses and certificates?

[2] Transportation Security Administration. TSA issues new cybersecurity requirements for airport and aircraft operators. March 2023. https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft

Control and reduce the asset attack surface

The fewer assets connected to airside and landside systems, the smaller the attack surface and the easier it is to defend.

Many organizations have assets on their network — or even whole network segments — that they don't see. In addition, with constant upgrades and construction projects underway at airports, systems that were once secure may now have vulnerabilities.

You can shrink the attack surface by segmenting airside and landside systems from other parts of the network and segmenting systems in areas that are undergoing construction. Segmentation policies and controls are now a TSA requirement.[3]

Other tactics include implementing firewalls and patching vulnerabilities. Where patches don't exist, find a compensating control that protects your systems.

Bottom line

Because understanding, controlling and reducing the attack surface is so complex, it's important to work with a vendor with deep expertise in attack surface management.

Questions to ask

- How do you ensure that networks are properly segmented?
- Have software developers, construction managers or other teams added network segments or devices without IT's knowledge and protection mechanisms?
- Which system assets are most at risk in the event of a cyberattack?

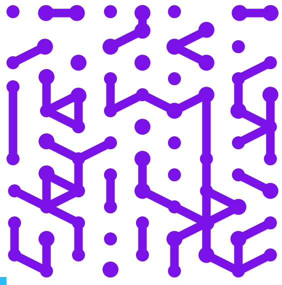
[3] Transportation Security Administration. TSA issues new cybersecurity requirements for airport and aircraft operators. March 2023. https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft

Manage asset vulnerabilities and prioritize by risk

It's vital to update software and patch devices quickly. However, the sheer volume of vulnerabilities can easily overwhelm even well-staffed IT organizations.

The number of accumulated vulnerabilities that organizations need to address today is in the millions. In addition, threat actors increasingly combine multiple known vulnerabilities in a single attack. The best way to prioritize vulnerabilities is to follow what threat actors are exploiting or are about to weaponize.

Known software vulnerabilities aren't the only form of risk to airport operations. You must also identify and address improper network segmentation, wireless security and other configuration issues.



Bottom line

The key to prioritizing vulnerabilities and issues appropriately is to understand them in context. Not all vulnerabilities present an imminent risk. Not all risks have the same potential impact. Choose solutions that use AI to prioritize alerts and offer contextual insights based on in-depth intelligence from billions of devices.

Questions to ask

- When assessing vulnerabilities, do you have the data you need, such as: What type of asset? Where is it located? How critical is it? Who owns it? Who manufactured it?
- Would this data improve your mitigation efforts?
- Do you have a process for prioritizing and remediating vulnerabilities?
- How do you ensure that all your endpoints are properly protected by endpoint security solutions (i.e., they have agents installed and agents are the correct version)?
- Do you have a growing backlog of vulnerabilities that need to be patched?
- Are you experiencing an increase in mean time to recovery (MTTR) metrics?
- Does Common Vulnerability Scoring System (CVSS) data provide little guidance on the criticality of risks to your business operations?

Detect threats and mitigate impacted assets early

The TSA requires organizations to implement continuous monitoring and detection policies and procedures.[4] This demands a network traffic analysis tool that gives you full visibility into every type of asset's behavior and uses AI and machine learning to alert you to potential threats.

"Airports must monitor the OT/IoT/IT ecosystem with precision and understand in real time how assets are behaving on the network," Yeager says. "Is a device pinging IP addresses that it shouldn't ping? Is it communicating outside of its assigned security level?"

Early-warning intelligence is essential to anticipate and mitigate cyber threats effectively. It is a key solution differentiator and includes:

Dynamic honeypots to attract threat actors and allow the observation of malicious behaviors.

Dark web intelligence that scours the deep and dark web for pertinent "chatter" about emerging threats.

Human intelligence incorporated through strategic feeds, reverse engineering and listening posts to enhance coverage and accuracy.

Bottom line

Choose a flexible and non-intrusive solution to passively monitor every device on your network, investigate suspicious activity and respond to incidents.

Questions to ask

- How do you detect asset behavior anomalies?
- What early-warning, evidence-based sources do you use to track threat actors and their activity?
- How do you integrate your various early-warning intelligence sources to get a unified view?
- When a threat is detected, how quickly can you pinpoint impacted assets?
- How easily can you block problematic devices from accessing the network?
- If you had all the data you need in a single view, would it improve your mean time to respond?

> *"The most useful part of Armis Centrix™ when it comes to OT is its ability to do raw network analysis. But that's not everything that Armis Centrix™ does. It also uses integrations and can collect data from our existing tools. The network mapper that uses the SNMP protocol can crawl around and quickly tell you that there's something connected to a switch."*
>
> **Christopher Peters,**
> Principal Architect, United Airlines.[5]

[4] Transportation Security Administration. TSA issues new cybersecurity requirements for airport and aircraft operators. March 2023. https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft

[5] Armis Case Study. United Airlines Uses Armis Centrix™ to Reduce OT Cybersecurity Risk. 2024. https://media.armis.com/pdfs/cs-united-airlines-en.pdf

Achieve, maintain and demonstrate compliance

Achieving compliance ensures airport authorities meet minimum criteria for security, functionality and accessibility. Demonstrating compliance is critical for defending against lawsuits.

“Airport authorities need to run instantaneous reports in order to meet these requirements without significantly taxing their IT and cyber teams, which are typically quite small,” says Yeager.

Bottom line

To achieve compliance and prove it, look for a solution that tracks and logs comprehensive activity for highly specialized devices that are unusual on most networks.

Questions to ask

- How do you ensure all your endpoints have required agents installed on them? How do you confirm the correct version?
- How do you validate that asset configurations meet internal policies?
- How do you demonstrate compliance across different assets?
- How do you track your overall security posture?
- Do you have the data you need to prove that your systems operate as required?

Asset Visibility, Vulnerability Prioritization

> Armis delivers comprehensive asset management and cybersecurity solutions that safeguard the systems used in airport operations. Armis Centrix™, the Armis Cyber Exposure Management Platform, is powered by the Armis AI-driven Asset Intelligence Engine, which sees, protects and manages billions of assets around the world in real time.

> By protecting the entire attack surface and managing cyber risk exposure as it occurs, Armis solutions ensure the critical infrastructure used in airport operations is secure and available.

Armis offers a depth of intelligence and technology that other vendors cannot match:

- **Flexible, non-intrusive, multi-detection and continuous asset management.** Armis Centrix™ understands every kind of device. It discovers, monitors and documents every single asset on the network and provides contextual intelligence about it.
- **Extensive, multi-faceted intelligence.** The Armis Collective Asset Intelligence Engine logs and analyzes more than 100 different types of activities across more than 5 billion devices. It's more than 10 times the size of all Armis competitors combined. In addition, it analyzes asset intelligence to comprehensively provide greater context about asset behavior and relationships.
- **Rapid deployment.** A single console provides a complete view and easy management of all assets — with zero configuration.

Armis Centrix™ for OT/IoT Security

Is tailored to protect OT and IoT devices in industrial, critical infrastructure and enterprise environments. It enables organizations to monitor and manage their OT/IoT ecosystems precisely and efficiently. Sophisticated policy, anomaly and behavior analysis capabilities provide early threat detection and proactive mitigation, minimizing the risk of cyberattacks and operational disruptions.

Armis Centrix™ for Asset Management and Security

Streamlines asset management processes while fortifying security posture. An intuitive interface and advanced analytics provide deep situational awareness and track and manage assets across diverse environments. Real-time threat detection and response safeguards assets from potential cyber risks and vulnerabilities.

Armis Centrix™ for VIPR Pro – Prioritization and Remediation

Closes the traditional gap between security findings, asset ownership and actionable remediation, offering a holistic and prioritized approach to exposure management. With VIPR Pro – Prioritization and Remediation, Armis goes beyond vulnerabilities to address security issues, misconfigurations in code, cloud infrastructure and applications.

Armis Centrix™ for Early Warning

Is the proactive cybersecurity solution designed to empower organizations with early warning intelligence to anticipate and mitigate cyber risk effectively. By leveraging AI-driven, evidence-based intelligence, Armis Centrix™ provides insights into the vulnerabilities that threat actors are exploiting in the wild or are about to weaponize, allowing organizations to understand their impact and take preemptive action.

Achieve Rapid Time to Value

Given aggressive cyberattacks, economic pressures and public scrutiny, airport authorities need powerful tools to protect passengers, avoid travel disruptions and meet regulatory mandates.

The Armis team can help you fully deploy and integrate an Armis solution across your landside and airside environments within days, if not hours. Get started now.

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.

1.888.452.4011

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo
Free Trial