NOZOMI NETWORKS

EBOOK

Airports: Cybersecurity for Operational Continuity & Compliance

Airports: Safety & Reliability First

Airports are the hub of global travel, collectively handling roughly 100,000 passenger and cargo flights a day.[1] Behind the scenes, an intricate web of IT, operational technology (OT) and Internet of Things (IoT) systems keeps everything running smoothly.

IT-related cyberattacks such as data breaches and ransomware certainly afflict airports. But it's the less protected OT and IoT systems that pose even greater risks. If attacked, the losses could threaten not only operational continuity but public safety.

Regulators know this. As critical infrastructure, airports must comply with the TSA Security Directives for aviation in the U.S. and the European Union's Network and Information Systems Directive 2 (NIS2), not to mention other regional regulations.

The challenge facing airports is to improve cyber and operational resilience while also meeting regulatory and corporate cybersecurity standards.

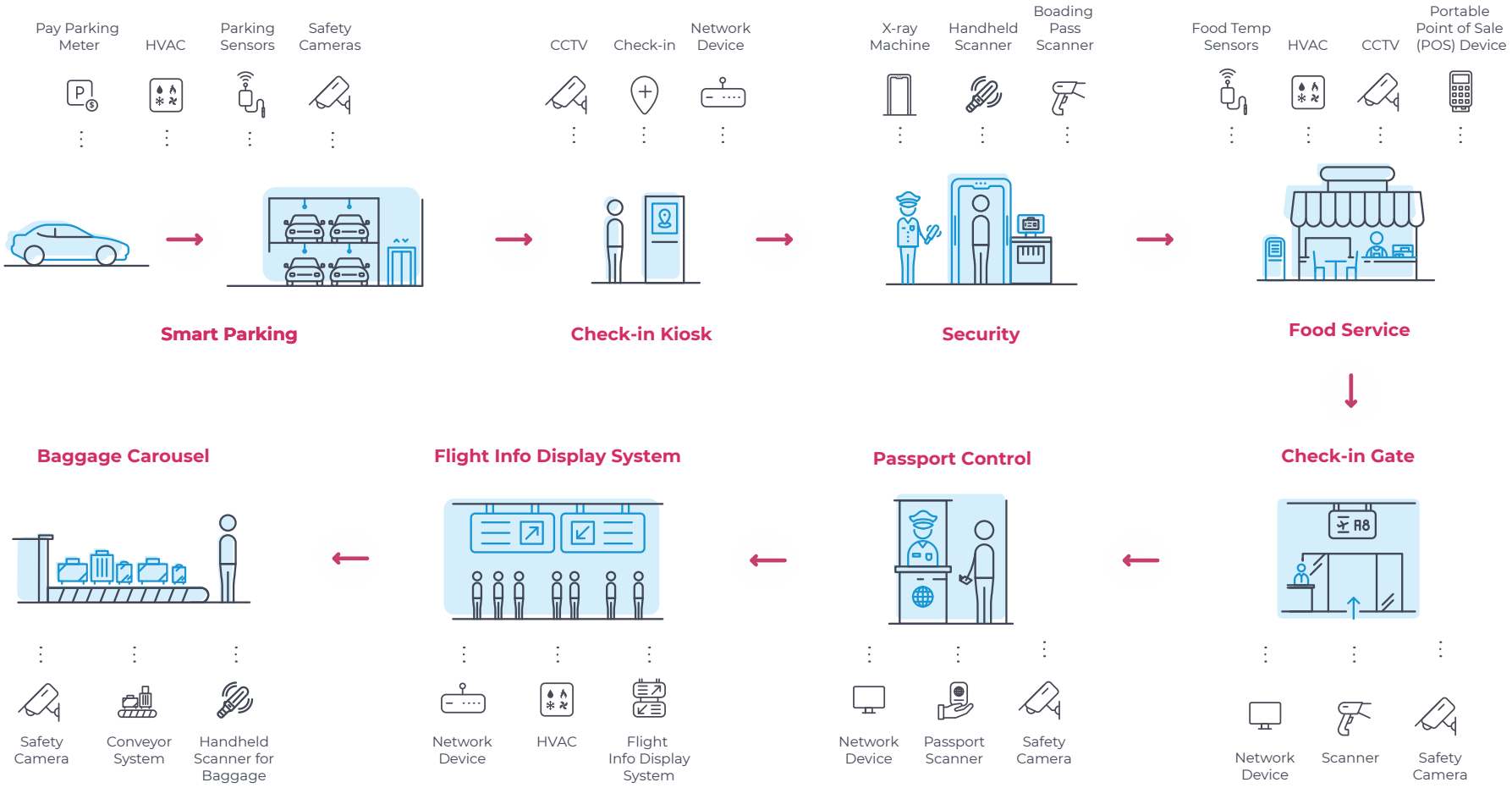
Nozomi Networks is the leading provider of visibility, vulnerability management and cybersecurity monitoring for airports.

We close OT/IoT security gaps, eliminate blind spots and help you meet regulatory and corporate cybersecurity standards.

[1] https://www.trip.com/ask/travel-questions/how-many-flights-per-day.html

The Connected Airport

From baggage handling and passenger screening to approach lighting and instrument landing systems, OT plays a crucial role in ensuring the safety, efficiency and reliability of airport operations.



The Challenge: Reducing Cyber Risk and Maintaining Operational Resilience

For airports, digital transformation is a double-edged sword. On one hand, it's the key path toward maintaining efficient and safe operations. On the other, it makes airports more vulnerable to cyber threats and disruptions.

With their complex web of interconnected OT, IoT and OT systems, airports need a solution that reduces cyber risk and improves operational resilience—at scale.

Airports need four major cybersecurity capabilities:

Asset inventory & vulnerability management

Regulatory & corporate standards compliance

Continuous cybersecurity & operational monitoring

Scalable & unified platform

While technological advancements have bolstered aviation safety, certain operational technology systems remain outdated and susceptible to cyberattacks.

TechForce, "Cyberattacks in the Aviation Industry," 2023

Asset inventory & vulnerability management

Converging OT, IoT and IT systems can lead to blind spots. Complex networks like those in airports may contain thousands of devices from various vendors, many of which are insecure by design, lacking key security standards. Cybersecurity teams must be able to overcome these obstacles to quickly pinpoint the greatest operational risks and keep planes flying.

The Nozomi Networks platform automates the discovery of all OT/IoT devices in your environment and captures detailed information about each to maintain an accurate asset inventory. It continuously identifies and scores open vulnerabilities on these devices, prioritizing the highest risks and providing actionable intelligence to aid remediation and reduce response time.

Legacy systems were not built to withstand today's sophisticated cyber threats.

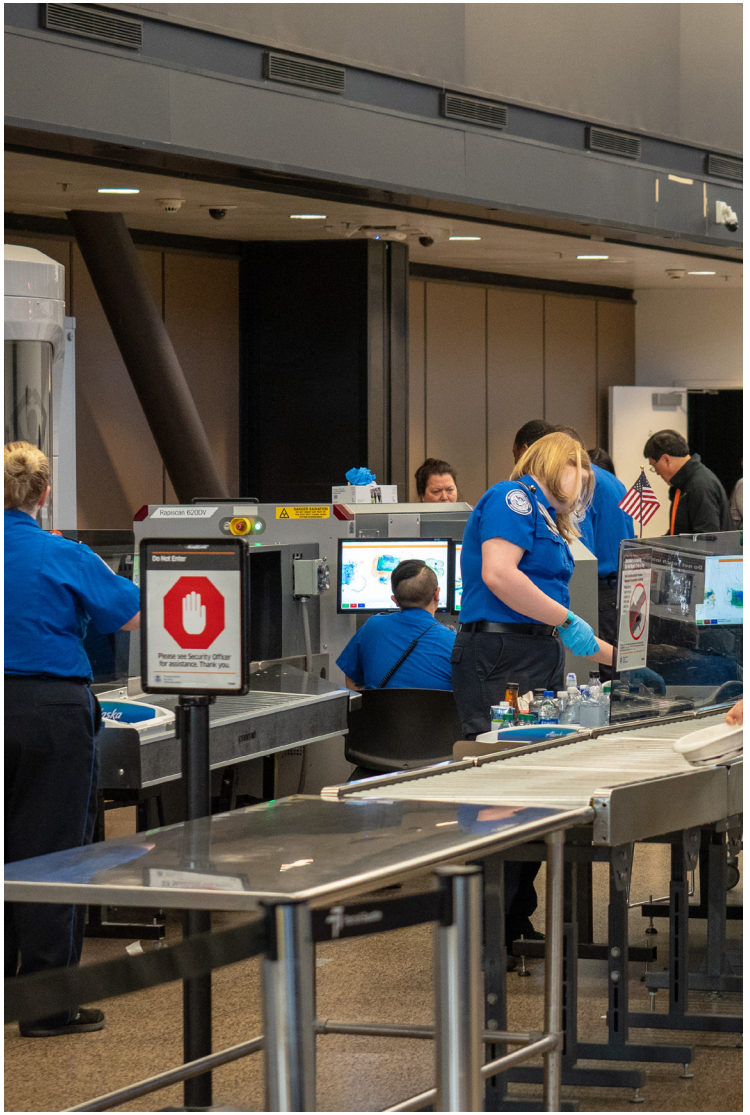
Regulatory and corporate standards compliance

In response to increasing cyber threats and incidents, cybersecurity requirements for airports are being tightened by regulators and legislators around the world. These include the TSA Security Directives in the U.S. and the NIS2 Directive in Europe, along with other country-specific laws and standards. Added pressure from governing boards has airport CISOs and cybersecurity teams focused on compliance across all systems and subsystems, including OT and IoT.

The Nozomi Networks platform provides asset inventory, vulnerability mapping and continuous security monitoring that aligns with the requirements in the TSA Security Directives. Likewise, it helps critical infrastructure operators align OT and IoT security practices with the seven broad security requirements in NIS2.

There were **39 major cyberattacks** in the aviation sector in the first half of 2023, **up 24% worldwide**.

Source: **KonBriefing**, **Resilinc**



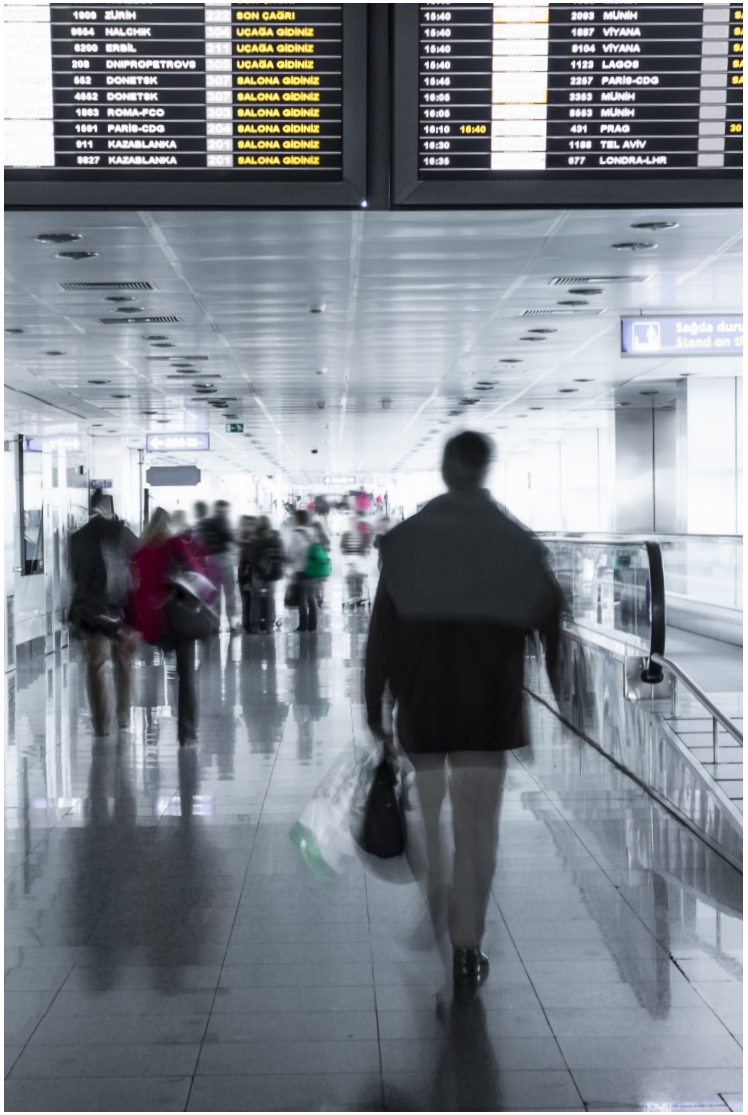
Continuous cybersecurity and operational monitoring

Airports are essentially micro cities that require continuous monitoring from every angle, including cybersecurity. To spot and troubleshoot networking and communication issues that threaten reliability, you need real-time visibility into your assets, connections, communications, protocols and more.

The Nozomi Networks platform provides continuous detection of threats, anomalies and vulnerabilities, enabling you to evaluate and address cyber and operational threats before they cause harm.

Using a combination of continuous network monitoring, endpoint monitoring and smart polling, it collects data about each asset's status and detects changes that could increase risk. AI-powered technology immediately baselines and profiles every device and its behavior to quickly pinpoint the security threats and process anomalies that matter most.

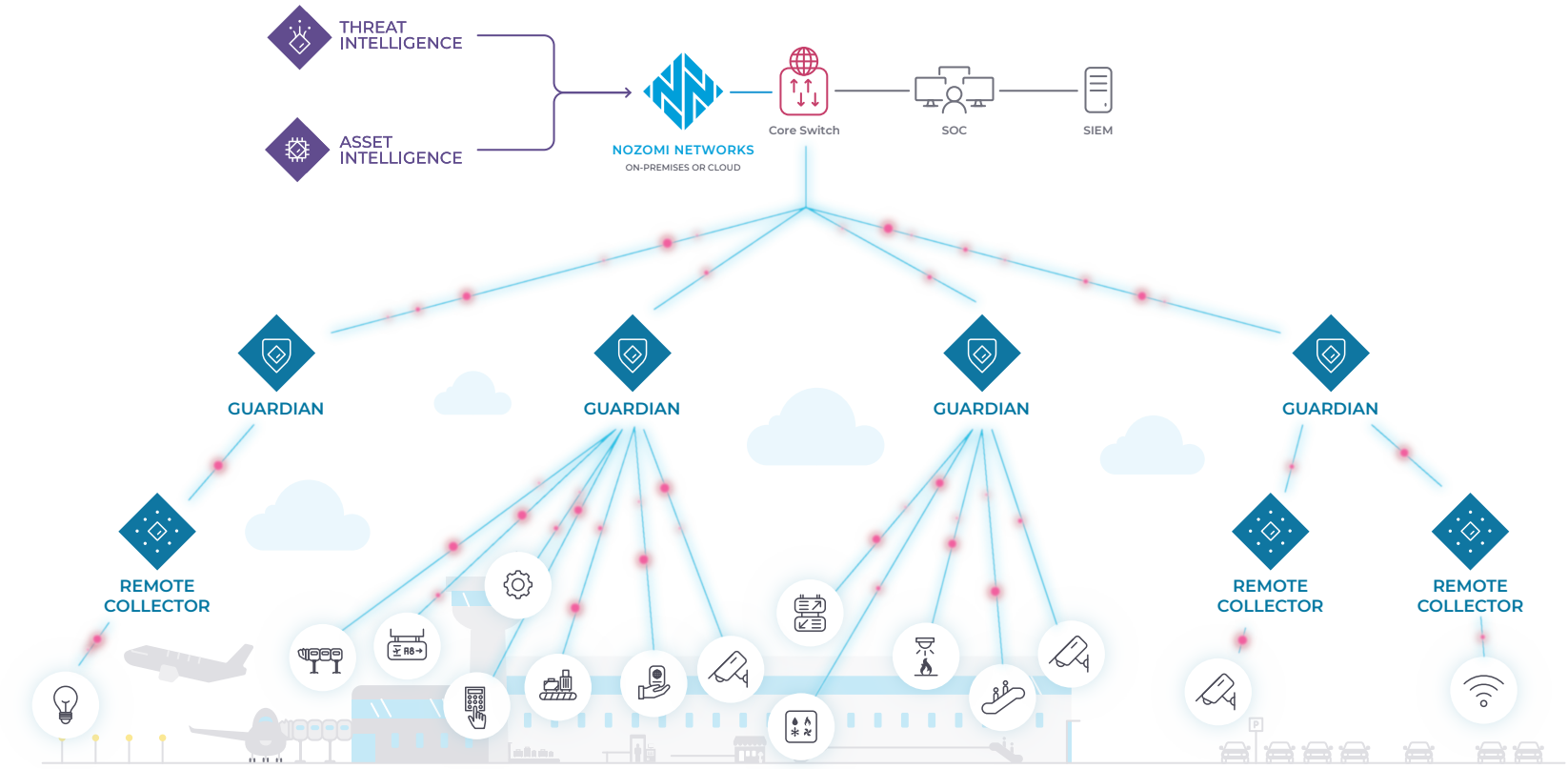
Airports have large attack surfaces with **high volumes of traffic** and **insufficient segmentation**.



Scalable and unified platform

Diverse and dispersed critical infrastructures require monitoring at scale. Simplify your multi-site deployment with a centralized, cloud-based solution that aggregates data and displays a comprehensive view of your entire network for timely analysis and action.

The Nozomi Networks platform unifies monitoring, assessment, detection and response across sensors and endpoints for an unlimited number of OT, IoT, IT, edge and cloud assets across sites, regions and teams.



CASE STUDY

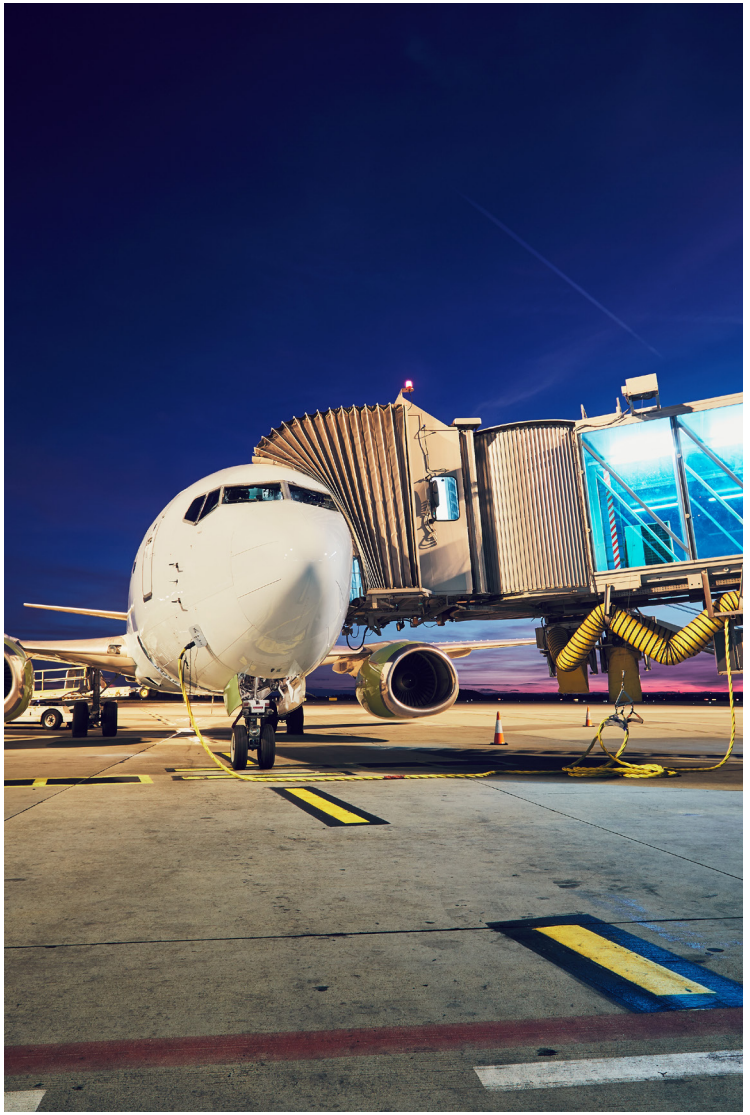
Top 5 Global Airport

Challenge

- Low visibility into diverse, complex mix of OT/IoT/IT systems and isolated networks
- High volume of traffic, variables and systems to be monitored
- Fragmented security analysis and delayed response due to disparate systems

Results

- Consolidated, real-time visibility across diverse systems and thousands of endpoints
- Prioritized, actionable insights into operational vulnerabilities and risks
- More efficient security analysis with operational asset and security data integrated into data lake, SIEM and SOC



NOZOMI NETWORKS

NEXT STEPS

Find out how Nozomi Networks can help you improve cyber resilience, visibility and security at your airport.

View Platform

Request a Demo

NOZOMI NETWORKS

Cybersecurity for OT, IoT and Critical Infrastructure

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

nozominetworks.com