NOZOMI NETWORKS

CASE STUDY

Top Five Global Airport Improves Visibility and Security

The Nozomi Networks solution allows this major airport to see its assets, improve vulnerability and security analysis, and quickly address cyber and operational risks.

Guardian Worked Out of the Box, and Produced Results in Only a Few Hours

Nozomi Networks Guardian was chosen after running a proof-of-concept play-off with two other vendor offerings. It was quickly evident that Guardian was able to meet our requirements, which were very much in the Identify phase of our OT security journey, and accompanied with excellent local support ...The OT protocol analysis was very impressive without any specific set up or training, was able detect machine behavioral changes over time. The accuracy of anomaly detection was very high, and was easily fine-tuned both by the Nozomi support and local OT and security teams.

Customer Profile

Top 5 Global Airport

EMEA Region

90,000 Employees

Goals & Challenges

Diverse and extremely complex OT, IoT and IT environments

Low visibility into the mix of OT/IoT/IT systems and isolated networks with high volumes of traffic

Multiple integrations required with 3rd-party systems, i.e., data lake/SIEM/SOC

Results

Consolidated visibility across diverse systems and thousands of endpoints

90% reduction in time to visibility into core airport systems

Real-time insights into OT/IoT vulnerabilities and risks

Improved security analysis thanks to seamless integration of operational data into data lake, SIEM and SOC

Nozomi Networks Guardian

Unlocks Visibility, Vulnerability Management and Security Monitoring for Complex Airport Systems

The Challenge:

Gaining visibility across diverse OT and IoT systems and integrating operational data into data lake/SIEM.

Airports are under tremendous pressure to secure highly diverse and dispersed networks from cyberattacks and incidents that could disrupt passenger services and operations. While this global airport was not directly required to comply with cybersecurity regulations, it wanted to measure up to industry best practices to ensure safety and security across their enormous threat landscape.

Protecting the airport's core operations required improved visibility across a complex and diverse mix of OT and IoT systems with high volumes of endpoints and network traffic. Another key priority was to improve security analysis and decision making through the integration of operational and security information into the data lake/SIEM. The airport included 20 separate systems containing >100,000 nodes with various protocols and integrations into third-party systems. To achieve their security objectives, the airport was looking for an open platform visibility and security solution that could scale across a huge environment and integrate with the data lake.

The Solution:

A highly scalable solution that provides visibility into core operations and seamlessly integrates with IT infrastructure.

Close to 20 Guardian sensors and multiple Central Management Consoles (CMCs) were deployed across three terminals, creating unified visibility into core airport OT and IoT systems, including the airport's Building Management System, CCTV, Emergency System, Fire Alarm System, X-RAY, AirOS, Baggage Handling System, Public Address System, Gate Operating Systems, and Catering Systems. The solution was delivered locally, scaled across an enormous environment, and integrated with the airport's data lake.

Even with multiple proprietary systems, Nozomi Networks supplied data flow diagrams, revealing communications between systems, and detecting anomalies. Thanks to its powerful ad hoc query tool, Nozomi Networks added custom rules to provide alerts and actionable insights so the airport could mitigate cyber and operational threats before they caused harm.

Nozomi Networks utilized industry-leading integrations with SIEM and SOC systems to bring missing operational data and contextual information into the airport's IT infrastructure for faster, more comprehensive risk reduction and incident response.

The Results: Unified visibility across complex environments and improved security decision making.

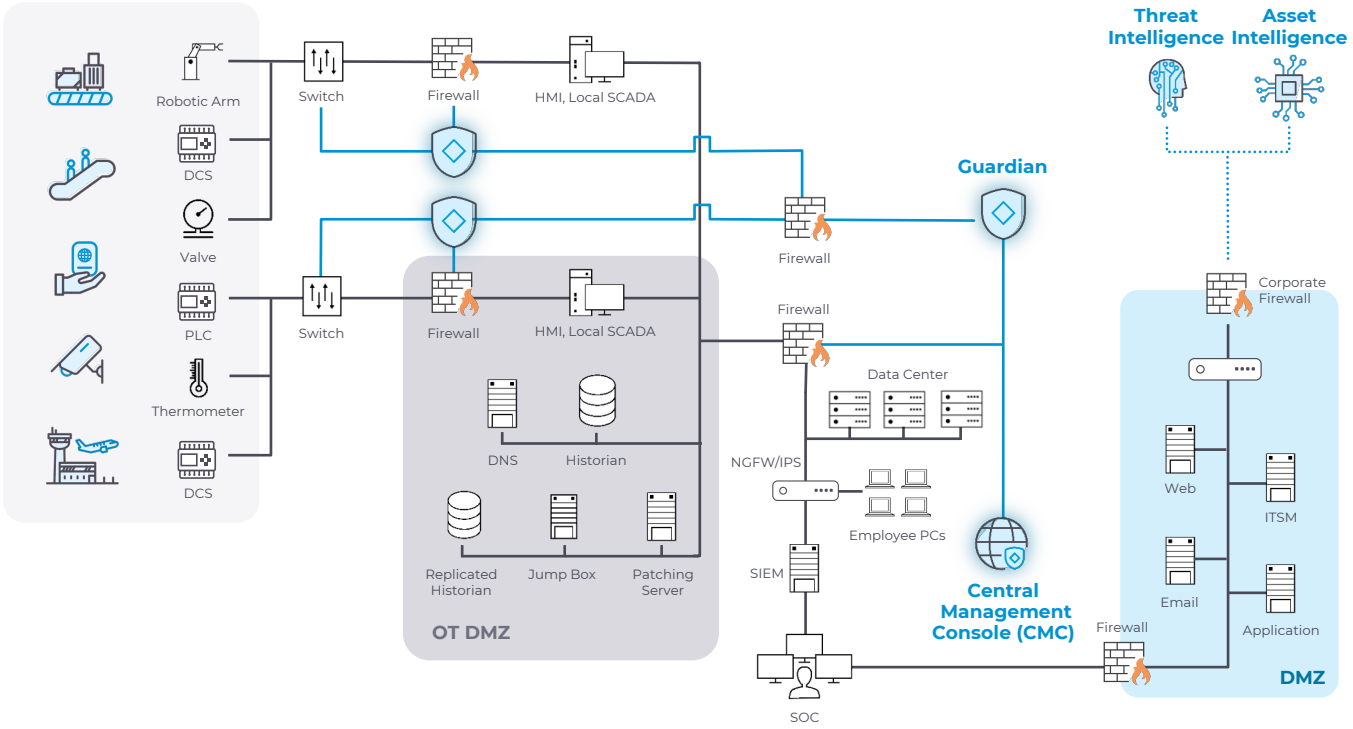
The deployment of Guardian generated an interactive network visualization map that displayed a consolidated view of the airport's core systems, reducing time to visibility by 90%.

Using the Nozomi Networks solution, the customer was able to normalize operational data and integrate it into their data lake. As a result, the customer was able to run analytics using comprehensive data for better decision making.

The airport was able to ensure security and improve KPIs with a scalable solution that provides visibility, assesses vulnerabilities, detects malware and gives advance notice of disruptions.

The Nozomi Networks solution enabled this top 5 global airport to manage cyber risk while innovating and adding new technologies.

90%
reduction in time to visibility.



Industrial Strength Cyber and Operational Resilience

With the Nozomi Networks solution you can protect a broad range of airport subsystems with rapid asset discovery, security monitoring and accelerated incident response. Deployment is readily tailored to meet your needs utilizing an extensive range of appliances, a SaaS application, a flexible architecture and integrations with other systems.

Other example deployment architectures, showing a Purdue Model or cloud components, are available. Simply visit nozominetworks.com

The Nozomi Networks Advantage

Nozomi Networks is the leading provider of visibility, vulnerability management and security monitoring for airports. Our scalability and flexible deployment options provide a range of coverage from individual subsystems to the largest of international airports with their many complex and critical systems. We close OT and IoT security gaps, eliminate blind spots, and help meet regulatory and corporate cyber security standards.

★★★★★

ROLE:
Infrastructure and Operations

COMPANY SIZE:
1B – 3B USD

Nozomi is very easy to use, and its information can be integrated easily into a SIEM.

We use Nozomi for analysis of our OT network and we appreciate a lot of feedback from the system and the fact that it is a very powerful system.

★★★★★

ROLE:
Security Risk Management

COMPANY SIZE:
250M – 500M USD

A CISO Must Have For OT Environment.

Nozomi Networks is the leader in this field. It's not just a security technology it's simply an eye wide open into the darkness world of the Operation technology. For me as Security Manager it's really a must have!!

More Reviews From Nozomi Networks Customers.

NOZOMI NETWORKS

Nozomi Networks

The Leading Solution for OT and IoT Security and Visibility

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

CS-AIR-Top-5-Global-Airport-8.5x11-002

nozominetworks.com