CASE STUDY FOR AIRPORTS' CONNECTED DEVICES

INTERNATIONAL AIRPORT MAXIMIZES SECURITY AND OPERATIONAL EFFICIENCY WITH **SecuriThings HORIZON**

Airports' efficiency is driven by security and safety which became fundamental for passengers alongside their overall experience. Accordingly, airports have made **major investments in physical security devices** such as video surveillance and access control, as well as smart systems such as face and license plate recognition to monitor behavior of an exponentially increasing number of passengers.

Managing these connected devices at scale has become a liability due to their **inherent vulnerability, physical accessibility and manual maintenance**. In fact, as any other IoT deployment, physical security devices are prone to failures and can be exploited by hackers to enter the broader network and access critical data. The challenge is even bigger as these devices are **remotely deployed within large distances** across multiple buildings and assets (e.g., terminals, parking, outdoors, etc.).

A service breakdown resulting from either cyber-attack or any operational issue on a single device could have severe consequences – from generating huge reputation damage to threatening lives.

PROTECT IoT DEVICES. MAXIMIZE OPERATIONAL EFFICIENCY.

A major international hub was facing a **lack of edge visibility and control** over thousands of deployed physical security devices (e.g. video surveillance, access control).

The dedicated team accountable for these devices had no way to **detect and mitigate cyber-threats** turning each device into a potential entry point to the network and data.

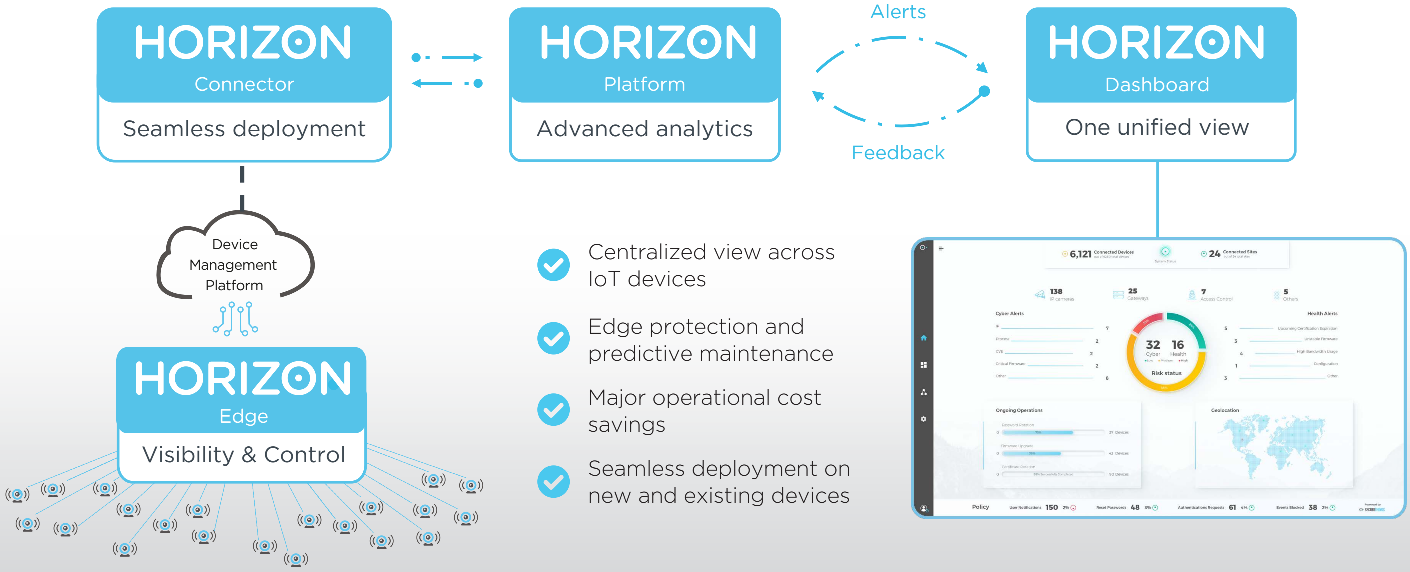
In addition, the team was challenged by the ongoing maintenance of these devices, performing most tasks such as fixing failures and upgrading firmware versions **manually and randomly**. This resulted in excessive time and cost.

The dedicated team sought a solution to maximize its operational and security efficiency.

SecuriThings Horizon Maximizes Airports' Security Efficiency

SecuriThings **HORIZON** is **the first IoTOps solution** automating the operational management of connected devices. The software-only solution provides risk detection, predictive maintenance and automated operations.

Horizon has been seamlessly deployed on existing and new video surveillance devices by connecting to the airport's central Video Management System (VMS). From that point on, Horizon is performing 24/7 monitoring and analysis across all devices.



- ✓ Centralized view across IoT devices
- ✓ Edge protection and predictive maintenance
- ✓ Major operational cost savings
- ✓ Seamless deployment on new and existing devices

Fast and Actionable Results

Immediately following deployment, SecuriThings **HORIZON** raised several high severity alerts and discovered multiple security risks:

- **12%** accessed by suspicious IPs on multiple ports
- **13%** running vulnerable or outdated firmware versions
- **10%** presenting significant health issues (unstable devices, stream disconnection, excessive resource consumption, etc.)
- **34%** affected by configuration issues (default credentials, multiple recording servers, etc.)
- **4%** with high-risk exposed services (FTP, UPNP, SSID, etc.)

Deploying SecuriThings Horizon, the airport has now **full visibility and control over its physical security devices** and is looking to expand the scope of monitored devices to additional IoT-enabled systems.

> **"Deploying SecuriThings HORIZON, we are now able to automate risk mitigation and benefit from predictive maintenance for our connected devices."**
>
> *Director of Physical Security, International Airport*