Flying High: Groupe ADP Elevates Its Network Security with Forescout

10,000

more devices than anticipated discovered on ADP's network

50%

enhanced operational efficiencies through comprehensive device data

1 Day

to achieve full visibility to devices connected to the network

Industry

- Air Transport/Airport Operations

Environment

- World's largest airport group by passenger numbers
- Over 35,000 devices identified on its network
- Thousands of employees spanning multiple global locations

Challenge

- Protecting against potential cyberthreats without hindering operations
- Lack of visibility to all connected devices
- Expansive, heterogeneous, and complex network environment
- Ineffective certificate-based security system

Overview

Groupe ADP (Aéroports de Paris) operates as one of the world's premier airport groups. The group handles millions of passengers each year with a vast portfolio that includes running three major airports around Paris and holding participation shares in various international airports, from Santiago to New Delhi. ADP sought a solution to secure its sprawling network infrastructure, encompassing many IT and OT devices. By adopting Forescout, Groupe ADP takes a major step in its cybersecurity journey.

> "With a growing network and increasing challenges in visibility, we sought a solution that could offer clarity and control. Forescout provided us not only with comprehensive visibility across our vast network but also the ability to enforce security policies without disrupting our operations—making it the perfect partner for Groupe ADP's complex environment."
>
> *— Eric Vautier, Group CISO, Groupe ADP*

Business Challenges

Airports are akin to mini-cities, housing an intricate web of complex and heterogeneous networks. Groupe ADP has three distinct networks:

- The corporate IT network, used for HR, email, and other business operations
- The airport network, which prioritizes high availability, powering check-in counters, boarding gates, and flight information displays
- The OT/IoT network, a complex mesh of baggage handling, lighting, security screening systems, and numerous sensors

- Rapidly changing networks outpacing monitoring capabilities
- Difficulty in classifying various device types
- Securing aging OT systems in terminals
- Keeping pace with increasing digitalization demands

Security Solution

- Forescout eyeSight
- Forescout eyeControl
- Forescout eyeRecover

Use Cases

- Network access control
- Device compliance
- Asset management
- Incident response

Results

- Discovered 35,000 devices—10,000 more than anticipated—in a single day
- Improved operational efficiency and reduced downtimes
- Enhanced communication between Groupe ADP's internal teams
- Boosted efficiency by preventing security vulnerabilities
- Ensured security remained uncompromised with a scalable solution

Operating in a complex environment, Groupe ADP faced a dual challenge.

First was the challenge of limited space. Groupe ADP couldn't build bigger terminals because of environmental concerns and other issues. Yet, more people were flying than ever before. As Eric Vautier, Group CISO pointed out, "Our physical limitations pushed us to think digitally."

By harnessing advanced technology solutions, Groupe ADP enhanced its operational efficiency within an airport's existing space. This digital transformation enabled better passenger flow management, more efficient flight scheduling, and optimized baggage handling, effectively serving more passengers without expanding the physical footprint.
But with increased modernization came the second challenge: cybersecurity. Potential vulnerabilities multiplied as Groupe ADP integrated more operational technology/Internet of Things (OT/IoT) devices to operate more efficiently. The organization was adding more touchpoints that could be exploited if not adequately secured.

"Networks at Groupe ADP are changing rapidly, and even our network team did not have full visibility to the devices connected to them," said Vautier. Previously, Groupe ADP attempted to bolster network security with certificates, but this approach fell short. It lacked the comprehensive visibility needed, was incompatible with several airport-specific systems and devices, and demanded extensive manual oversight.

"Relying solely on certificates misses the bigger picture; they don't tell us about compliance, the current security stance, or even what a device is actively doing," Vautier explained. The pressing issue? Addressing problems became increasingly difficult without the ability to check a device's integrity.

Why Forescout?

Recognizing the need for a more dynamic solution, Vautier and the Groupe ADP team turned to Forescout. Moving beyond traditional certificate-based methods, they opted for a solution emphasizing the complete visibility of all connected devices. This logical step with Forescout not only addressed Groupe ADP's unique challenges but also positioned them at the forefront of network security in large-scale operations.

Soon, the need for better collaboration across the organization became apparent. "In our complex environment, trust and teamwork are paramount," Vautier remarked. "With Forescout's tools in place, Groupe ADP's network, IT, and cybersecurity teams found common ground." This approach ensured alignment among all stakeholders, reinforcing trust and facilitating informed decision-making.

Moreover, Forescout's "crawl, walk, run" approach resonated with Groupe ADP. For Vautier and the teams he oversees and interacts with, a phased, orderly implementation was essential. He wanted to ensure that everything functioned properly at each stage without causing disruptions to operations at the airport, which relies on the 24/7 availability of its systems.

Groupe ADP first deployed Forescout at the IT building. When the network, IT, and security teams saw everything was working as it should, they branched out to the airport IT network, implementing Forescout, step by step, at each terminal. Vautier noted: "Starting with our IT building allowed us to test the waters, ensuring that the system was robust and reliable before rolling it out to our critical airport terminals."

Business Impact

Enhanced Network Visibility and Device Identification

One of the immediate impacts of the Forescout implementation was the comprehensive visibility it provided. In just a single day, Forescout discovered nearly 35,000 devices on the network—10,000 more than they had anticipated. It also shed light on potential vulnerabilities, which could then be addressed and remediated promptly.
After the asset discovery phase, Groupe ADP leveraged Forescout's multi-dimensional classification taxonomy for traditional, IoT, and OT devices to identify device function and type, operating system and version, vendor and model, and more. With this detailed information, Groupe ADP could remediate issues faster and make better security choices.

"Forescout gave us the depth of insight we never had before, transforming our approach from guesswork to precision," Vautier observed. This depth of understanding was not possible with the legacy certificate-based solution.

Improved Collaboration

Vautier strategically harnessed Forescout to enhance communication between network and IT departments. By introducing these capabilities, the network team emerged as pivotal players, adeptly configuring, monitoring, and overseeing daily functions. They could now easily identify devices on the network and gauge their activity.

Meanwhile, the airport IT team leveraged Forescout to monitor device security and detect rogue devices. This collaborative approach ensured a unified, efficient implementation, fostering a cohesive environment where both teams could work in sync.

Enhanced Security Monitoring

With Forescout, Groupe ADP swiftly classifies and controls devices, significantly enhancing its security posture. The refined categorization and vigilant monitoring of devices have substantially reduced potential downtime and disruptions.

Increased Efficiency

By adeptly managing potential security threats, Groupe ADP has boosted performance efficiency. By proactively preventing disruptions, Groupe ADP has not only maximized its operational hours, but has also ensured consistent passenger satisfaction. This time-efficient approach is further bolstering Groupe ADP's esteemed reputation.

Scalable Solution

As Groupe ADP continues its digital transformation journey, Forescout's solution offers scalability to accommodate growth. "As our network evolves, Forescout's adaptability becomes even more crucial," said Vautier. This ensures the organization maintains a strong security posture as the network grows and diversifies.

Vautier's vision for the near future is to deploy Forescout in the OT/IoT network and take a deeper dive into Forescout's classification and categorizing to enhance the quality of device data for faster detection and remediation of potential issues.

Groupe ADP's relationship with Forescout represents a successful partnership in the ever-evolving realm of cybersecurity. It underscores the importance of visibility, collaboration, and adaptability in creating a secure and efficient network environment.

Forescout Technologies, Inc.

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com