Case Study

FORESCOUT

Mobility ADO

Global Transportation Company Trusts Forescout to Actively Defend Its Enterprise of Things

$6.4M
saved in first-year efficiency benefits

3 DAYS
to implement device compliance

99%
compliance across all devices

MOBILITY ADO®

Industry
Transportation

Environment
38,000 wired and wireless devices across 15 sites—and continuing to grow through acquisition; 26,000 employees

Challenge

- Minimize risk of data breach or disruption of business continuity
- See all devices on a highly distributed network, including IoT and employee-owned
- Implement security governance to actively defend all these endpoints

Overview

Mobility ADO is a rapidly growing global provider of bus, metro, railway, taxi and other transport services, with a presence in eight countries in Central and South America and Europe. Deploying the Forescout platform has enabled the company's small security team to actively defend all the devices on its highly distributed network—from PCs and tablets to point-of-sale ticketing and mobile tracking devices. The team relies on the Forescout solution to provide robust network access control (NAC), continuous device compliance monitoring and assessment, dynamic network segmentation, automatic remediation, and more. Estimated savings from business benefits total millions of dollars each year.

Business Challenge

"As we looked for ways to implement governance, NAC was a top priority, but NAC was only a piece of the continuous adaptive protection we needed."
— Hector Mendez, Chief Security Officer, Mobility ADO

Customers depend on Mobility ADO's business 24x7x365, so business continuity is essential. But the company's highly distributed, geographically dispersed enterprise; wide range of Enterprise of Things devices (corporate, IoT, and employee-owned since so many employees are now working remotely from home) and tremendous growth by acquisition exacerbated the difficulty of minimizing the risk of business disruption. Also, Mobility ADO must keep personal information safe and comply with PCI. To address these challenges, the company needed NAC, but it also required the means to keep devices compliant, more easily spot and protect vulnerabilities, improve incident response and accelerate remediation—in short, to defend all its endpoints more proactively. All with a security team of three.

Security Solution

- Forescout platform
- Forescout eyeExtend for Palo Alto Networks Next-Generation Firewall

Use Cases

- Network access control
- IoT security
- Network segmentation
- Asset inventory
- Device compliance
- Security orchestration

Results

- Significant ROI—$22.6M USD savings estimated over three years—from IT staff efficiency and business productivity benefits
- Real-time, comprehensive visibility across all network-connected things
- 99% device compliance
- Patching pushed out in days rather than months
- Block network access to rogue and noncompliant devices and automatic remediation when possible
- Proactive, automated NAC policy enforcement
- Faster incident response, quickly discovering ransomware attacks and isolating devices to prevent damage
- Accurate, real-time asset inventory is source of truth for all—including the managed services provider
- Automated sharing of real-time device context with multivendor tools for greater efficiency and effectiveness

Why Forescout?

With NAC topping Mobility ADO's priority list, Chief Security Officer Hector Mendez chose the Forescout platform for device visibility and control, in large part because of the solution's leadership position in Gartner's Market Guide and agentless approach. However, upon implementing the Forescout platform—which was fully deployed across the entire global enterprise within three weeks—Mendez and his team immediately realized the benefits of real-time, comprehensive discovery extended far beyond NAC. Furthermore, the first time the company was attacked by malware after implementing the Forescout platform, they recognized the solution's potential for accelerating incident response.

> "Forescout gives us more than visibility across devices; it gives us governance. I don't have to trust that everyone is doing the right thing because I can see what is happening and proactively enforce rules to maintain control of our environment."
>
> — Hector Mendez, Chief Security Officer, Mobility ADO

Business Impact

Device Compliance of 99% and 100% Accurate Asset Inventory

One of the first things Mobility ADO's security team discovered after implementing the Forescout platform was that most of the company's user devices were not fully compliant with up-to-date patching or current, functioning antivirus protection. "Instead of the two to three months that our managed services provider said it would take to bring all our devices up to date, with Forescout, we pushed out patches and current antivirus software across our entire global enterprise in three days," notes Mendez. "Today, our devices are 99% compliant on patching and antivirus protection. Using Forescout to identify and classify all devices also gives us a more accurate inventory than ever before. Today Forescout provides the last word, even for our managed services provider."

Dramatically Improved Security Governance with NAC and Network Segmentation

Mendez and his team use information from the Forescout platform to provide greater control and improve Mobility ADO's security posture. Using Forescout data, they closed all ports that do not need to be open and enforced policies to cease unnecessary communications between servers and other devices. The Forescout solution also blocks access to rogue or noncompliant devices. If a user with a noncompliant device attempts to connect, the Forescout platform blocks it, scans the machine and automatically tries to remediate to achieve compliance. In addition, the Forescout platform automatically identifies and classifies devices attempting to connect to Mobility ADO's network and assigns them to the appropriate VLAN to minimize potential breach impact and facilitate PCI compliance.

> "In short, Forescout is the front line of our active defense. It gives us the information we need to make smart decisions about security as well as infrastructure and operations."
>
> — Hector Mendez, Chief Security Officer, Mobility ADO

Faster Detection and Incident Response

Mendez and his team have used the Forescout platform to stop ransomware and denial-of-service attacks in their tracks several times. "When the Forescout platform detects abnormal behavior, we block the affected device or devices, investigate and immediately create a rule to prevent the behavior elsewhere," explains Mendez. "With Forescout, we have quickly squelched ransomware before it could do serious harm. And anytime we learn of a new vulnerability we immediately implement rules to prevent hackers from taking advantage. Such proactive prevention has kept us from being impacted by numerous vulnerabilities including WannaCry and Ripple20."

Millions of Dollars of ROI Benefits

To quantify Forescout's economic value to ADO Mobility, Mendez used a customer-based ROI tool developed by IDC. The ROI analysis showed $6.36 million first-year savings and $22.6 million three-year savings, primarily from staff efficiency benefits and business productivity gains but also from risk mitigation and IT infrastructure cost reductions. In addition to increasing operational efficiencies through automation, integrating the Forescout platform with existing tools has enhanced the value of those tools by providing them with accurate, real-time, contextual information about everything on the network.

"In short, Forescout is the front line of our active defense," says Mobility ADO CSO Mendez. "It gives us the information we need to make smart decisions about security as well as infrastructure and operations."

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

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

Learn more at Forescout.com