Case Study

FORESCOUT

NJ TRANSIT

Boosts Cybersecurity Efficiency and Effectiveness with Forescout Platform Capabilities and Integrations

1 WEEK
to achieve core enterprise visibility

HOURS
saved daily from automated compliance and remediation

6,000
unknown devices discovered

NJ TRANSIT The Way To Go.

Industry
Government

Environment
16,000 wired and wireless devices across 270 locations; 10,000 employees; campus, data center

Challenge

- Maintain and track compliance of all devices on the network, including IoT
- Comply with PCI as a Level 1 merchant
- Control network access and protect endpoints across 270 field sites

Security Solution

- Forescout platform
- Forescout eyeExtend for Check Point® NGFW
- Forescout eyeExtend for IBM® BigFix®
- Forescout eyeExtend for McAfee® ePO™
- Forescout eyeExtend for Qualys® VM
- Forescout eyeExtend Connect

Overview

NJ TRANSIT is a state-owned public transportation system that operates bus, light rail and commuter rail services throughout the U.S. state of New Jersey as well as into New York and Philadelphia. By using the Forescout platform for device visibility and control and integrating it with a range of security tools in their environment, the NJ TRANSIT's cybersecurity team did more than just meet their visibility and NAC objectives. They also dramatically improved the organization's overall security posture and realized significant time savings thanks to automated device compliance checks, reductions in remediation activity, easier audit reporting, and other efficiency improvements.

Business Challenge

"First and foremost, you need to know what you have [on your network] so you know what is and isn't protected."
—Bilal Khan, Chief Technology and Security Officer, NJ TRANSIT

NJ TRANSIT's security team strives to provide customers with uninterrupted service as well as protect the organization's assets and customers' personal information. "Knowing what is on the network is critical. But as devices have proliferated over time—including many agentless IoT devices such as HVAC and wastewater management systems, payroll clocks, printers, and so on—knowing what is on the network had become increasingly difficult," says Lookman Fazal, NJ TRANSITS chief information and digital officer. The potential for rogue devices at any of the 270 field sites was a major concern as was keeping managed devices compliant with both internal security standards and federal regulations. NJ TRANSIT is classified as a PCI DSS Level 1 merchant and because it has a medical unit and police force, it is also subject to HIPAA and CJIS regulations.

Use Cases

- Device visibility
- Network access control
- Incident response
- Device compliance
- Regulatory compliance

Results

- Rapid time to value—one week to achieve a high degree of visibility across the network
- 60% more devices discovered on network than expected
- Accurate, real-time asset inventory system to replace cumbersome, incomplete manual method
- Hours saved daily due to reduced remediation and troubleshooting
- Stronger security posture from dramatically improved and automated device compliance
- Network access control (NAC) that allows only authorized devices to connect, including thousands of employees working remotely
- Accurate, granular data to accelerate remediation, incident response and decision making

> "When we start enriching data from other tools with accurate, real-time data from Forescout, our cybersecurity team is able to make data-driven decisions with confidence. It allows me to sleep at night."
>
> — Bilal Khan, Chief Technology and Security Officer, NJ TRANSIT

Why Forescout?

"Beyond NAC, we were looking for a product that would give us reliable, comprehensive visibility that would show us what we did not know," recalls John Franciscone III, NJ TRANSIT's director of cybersecurity. "When we watched our first Forescout demo, we knew it was going to be a home run product for us…the way it interacts with the network, providing accurate, real-time data and granular host inspections that far and away surpass anything else out there."

Business Impact

Time to Value in One Week, 60% More Devices Discovered than Expected

A 30-day Proof of Value (PoV) of the Forescout platform that morphed into full production mode before the month ended validated the NJ TRANSIT security team's initial impressions. Within the first week of the PoV, NJ TRANSIT had complete visibility across all but a small fraction of its infrastructure. In the past, creating an asset inventory was a very manual process highly dependent on an agent-based patch management tool. Using this process, the team had been aware of 10,000 devices scattered across NJ TRANSIT's network. In addition to those 10,000 known devices, the Forescout platform discovered an additional 6,000 devices. "Now our asset inventory comes directly from the Forescout dashboard," says Franciscone. "Unlike before, it is easy to obtain and we can trust that it is accurate."

Transformed Security Posture Thanks to Integrations and Automation

The NJ TRANSIT security team also overhauled device compliance. The Forescout platform continuously checks and reports on the status of Windows configurations, antivirus and disk encryption for all managed devices on the network. But that's not all thanks to integration of the Forescout platform with McAfee ePO. If the McAfee agent is installed on an endpoint but not communicating properly, the Forescout solution automatically informs the McAfee ePO console, which then initiates a script to restart the system, and, if that does not fix the problem, reloads the antivirus software. In addition, Forescout data fed into NJ TRANSIT's Qualys vulnerability management system enhances vulnerability detection. The cybersecurity team is also integrating CrowdStrike endpoint detection and response software with the Forescout platform via Forescout eyeConnect to add a lot more context to accelerate incident response. "When we start enriching data from other tools with accurate, real-time data from Forescout, our cybersecurity team is able to make data-driven decisions with confidence. It allows me to sleep at night," says Bilal Khan, NJ TRANSIT's chief technology and security officer.

"Know-It-All NAC"

With COVID-19, many more NJ TRANSIT employees than usual are working from home, connecting to the network via VPN. The Forescout platform checks all their devices and any others as they try to connect to the network, blocking access if they are not authorized and complaint. "Forescout is basically the bouncer that decides who gets in and who doesn't," explains Jonathan Cassidy, NJ TRANSIT's lead cybersecurity analyst. "Thanks to the Forescout-Check Point integration, you don't get past our firewall until Forescout lets you. We call it know-it-all NAC. It ensures that every device and every IP address on our network has a purpose, that we have no useless, unneeded, or risky devices connected."

> "Knowing what is on the network is critical. But as devices have proliferated over time—including many agentless IoT devices such as HVAC and wastewater management systems, payroll clocks, printers, and so on—knowing what is on the network had become increasingly difficult,"
>
> — Lookman Fazal, Chief Information and Digital Officer, NJ TRANSIT

Operational Time Savings in Multiple Areas

Besides dramatically improving security posture with full visibility, continuous device posture assessment and NAC, the NJ TRANSIT security team has reaped significant operational time savings from using the Forescout platform. For instance, they now spend far less time on compliance reporting and internal and regulatory audits. Creating a list of PCI assets now takes minutes as opposed to a day or two. Pushing out patches and software updates is much faster and easier too.

But the most significant time savings is due to a huge reduction in remediation activity, in part because the team integrated the Forescout platform with its IBM BigFix endpoint management software. "In the past, something as simple as restarting a device could take hours, but now it takes only seconds," notes Cassidy. "Most of the time, Forescout silently takes care of things for us. I spend hours less time each day on remediation and troubleshooting."

Given the numerous benefits that NJ TRANSIT has reaped by implementing and integrating the Forescout platform, Franciscone has become a huge fan. "The Forescout platform has proven its value repeatedly and there's still so much more we can do with it," he says to peers. "Whether your team is large or small, do yourself a favor and check it out."

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

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at www.Forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners. Version 07_20