Case Study

FORESCOUT

Large U.S. City

Unified IT-OT Security Helps this Smart City Reduce Risk

1 MONTH
to full deployment

$400,000
annual savings from automation

COMPLETE
visibility of IT, IoT and OT

Industry
Government

Environment
3,000 wired and wireless devices spanning 23 locations (data centers, offices and backhaul facilities) throughout the city (population 120,000); 1,100 employees

Challenge

- Incomplete visibility into all connected devices, including agentless IoT and OT devices of all kinds
- Incident response delayed by lack of security tool integration
- Small security team with limited time and resources

Overview

Community leaders in this American city of 120,000 people take pride in the city's diversified economy and its commitment to digital transformation. As part of its IT infrastructure, this smart city had accumulated an extensive and growing inventory of agentless IoT and OT devices to help deliver critical services. It lacked visibility into all connected endpoints and faced challenges controlling network access based on compliance with the city's strict security standards. Implementing the Forescout platform and Forescout eyeExtend modules meets the city's network access control (NAC) needs, provides comprehensive real-time visibility and enables integration and automation between myriad security software tools. Business benefits include savings of $400,000 annually from automating security tasks.

Business Challenge

"Our network simply cannot go down. We need robust NAC and security tools that maximize detection and prevention and accelerate incident response."
— Chief Information Officer, Large U.S. City

For its size, this city has a highly automated and intelligent network environment. A technical staff of three oversees network operations and approximately 3,000 endpoints across more than 20 locations. Included in those 3,000 endpoints are a wide assortment of IoT devices—everything from first responder communications equipment and safety cameras to timecard machines, HVAC systems and parking meters—that is growing at an unprecedented rate. In addition, the city's network staff must also track a growing number of operational technology (OT) devices, such as sewage and wastewater sensors. All these devices connect to an extended network that is the cornerstone of dependable 24x7x365 essential city services. Such a network requires sophisticated security and automated, orchestrated incident responses with as little delay as possible.

Security Solution

- Forescout platform
- Forescout eyeExtend for Palo Alto Networks® Next-Generation Firewall
- Forescout eyeExtend for Palo Alto Networks WildFire™
- Forescout eyeExtend for Tenable® Vulnerability Manager
- Forescout eyeExtend for VMware AirWatch®
- Forescout eyeExtend Connect

Use Cases

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

Results

- Rapid time to value: end-to-end deployment in one month
- Real-time visibility into all devices the instant they connect to the network
- Ability to ensure that connecting devices adhere to the city's internal controls
- Added value to existing investments by orchestrating and automating security tasks
- Ability to do more with limited budget and staff
- Accurate reporting of PCI and CJIS compliance while exceeding NIST requirements
- Estimated savings of $400,000 annually through automation

Why Forescout?

"When I came to the city, I wanted us to take security to another level before we experienced a security event," says the city's chief information officer. "Consequently, we acquired the Forescout platform early on to help fortify our security posture. We conducted a 'bakeoff' between Forescout and a few other competitors and we quickly discovered that we preferred the Forescout philosophy and flexible approach."

Time to value was also important. "We finished our end-to-end deployment with most of our rules in place in about a month," says the CIO. "Establishing what assets exist in the city was also quick, as was integration that let us assess the security footprint of things that are coming into the city."

> "Forescout has helped immensely with knowing which devices are on the network, understanding where they are located and their security posture and being able to ensure that they adhere to our internal controls."
>
> — Chief Information Officer, Large U.S. City

Business Impact

Comprehensive Device Detection and Assessment Plus NAC

With so many IoT assets to manage, using 802.1X was no longer viable for the city. The 802.1X-agnostic Forescout platform lets them detect and classify the city's broad range of agentless IoT devices as well as helps staff detect and better understand connected OT systems serving the city's sewage and wastewater systems. With the Forescout platform, they also easily detect devices with noncompliant or nonoperational antivirus software and out-of-date or end-of-life operating systems. The solution alerts city IT staff about noncompliant systems and blocks them from the network.

Enforcing Compliance and Reducing Incidents

Understanding the compliance posture and controlling every device that connects to your network is essential for ensuring network security. The Forescout solution's automated policies quickly discovered and shut down illicit hubs as well as switches that employees plugged in and used to expand network ports. "Forescout has helped us improve our security posture to the point where we no longer chase internal incidents," notes the CIO. "Today when an end user tries to connect an unauthorized device, the Forescout platform automatically blocks them and lets us know."

Boosting ROI and Security Operations Productivity

To extend the value of the Forescout platform even further, the city implemented Forescout eyeExtend modules that integrate the device visibility and control platform with the city's existing security tools, including:

- Palo Alto Networks® NGFW – The Forescout platform exchanges real-time device and user information with the city's next-generation firewalls. This lets the city automatically segment and enforce security policies based on rich device context, regardless of device type.

"We finished our end-to-end deployment with most of our rules in place in about a month. My previous deployment with a competitive product took us a year to get a lot of the rules in place and then the project fell flat on its face because it was too difficult. Forescout has been the 'Apple of NAC.' It is just that easy."

— Chief Information Officer, Large U.S. City

- Palo Alto Networks WildFire™ – The combination of WildFire's advanced threat intelligence and detection with Forescout's network-wide visibility and control enables rapid identification, containment and resolution of threats.
- Tenable® VM – The Forescout platform scans new devices as they join the network, which then triggers the Tenable vulnerability management system to scan at regular intervals. Unpatched devices or those that are otherwise noncompliant with the city's policy are quarantined.
- VMware AirWatch® Mobile Device Management – Integration with the Forescout platform helps IT administrators streamline the process of provisioning, managing and securing smartphones and tablets, all from a single portal.

Integrating the Forescout platform with existing security tools has also freed up the city's security team for more strategic tasks and positively impacted staffing requirements. "In personnel costs alone, we are saving $400,000 a year because the Forescout platform enables us to have the right automation and integration," says the city's CIO. "Forescout is a powerful partner."

Future Uses and Forescout Platform Benefits

The city's IT team feels like they have just scratched the surface of the Forescout platform's potential. The Forescout platform has already proven its worth beyond the security realm and is being used in other operational areas, such as network management. For instance, operational staff is currently looking into integrating NetFlow data into Forescout from the city's switches in order "react more intelligently to events." They are also evaluating using the Forescout platform for more dynamic segmentation and assessing the capabilities of Forescout SilentDefense™, which extends greater situational awareness and risk assessment into OT networks and critical infrastructure.

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