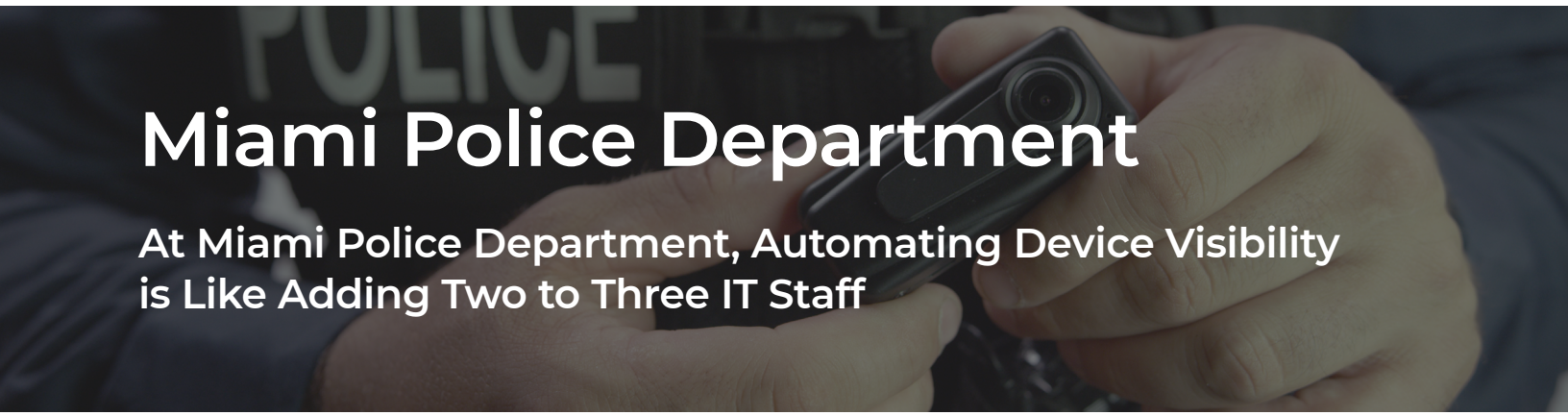
Case Study

FORESCOUT



Miami Police Department

At Miami Police Department, Automating Device Visibility is Like Adding Two to Three IT Staff

3 DAYS
to achieve enterprise visibility

HOURS
saved daily from automated compliance checks and remediation

DAYS
saved each month in software updates

Industry
Government

Environment
2,000 wired and wireless IT and IoT devices across campus, data center and police vehicles; 1,800 employees

Challenge

- Lack of visibility into all devices on network
- Time-consuming, fragmented approach to asset identification and compliance
- Limited IT staff
- High-profile events such as the Super Bowl make organization a strategic target for hackers

Security Solution

- Forescout platform
- Forescout eyeExtend for McAfee ePO
- Forescout eyeExtend for Palo Alto Networks WildFire

Overview

The Miami Police Department (MPD) works diligently to serve a city of over six million people. Implementing the Forescout platform has provided the MPD with the 100%, real-time visibility needed to know not only what devices are on their network—from laptops and ToughBooks to bodycams and license plate readers—and where they are located but how compliant they are. By automating manual processes related to device visibility and compliance, the organization's IT team has made the MPD safer while saving hours daily. They have also laid the foundation for robust network access control and increased efficiencies from integration with security tools.

Business Challenge

"The first tenant of cybersecurity readiness is understanding what's on your network, but verifying and managing assets and device hygiene simply took too long and was always incomplete."
— Joseph Pontillo, Information Systems Manager, Miami Police Department

Joseph Pontillo, the MPD's information systems manager, and his staff of 11 are responsible for all of the department's IT needs, including cybersecurity. To identify, audit and manage devices and device hygiene, his team relied on a "hodge podge" of existing tools, techniques and open source applications. However, this fragmented approach never yielded the comprehensive visibility or accurate asset inventory needed to enable network access control and secure the organization's network. Having limited staff only exacerbated the challenge. In addition, high-profile events occurring in Miami, such as Super Bowl LIV, made the organization an even more attractive target for malicious actors.

Use Cases

- Device visibility
- Device compliance
- Asset management

Results

- Rapid time to value—three days to achieve a high degree of visibility across the network
- Accurate, real-time asset inventory replaced time-consuming, incomplete manual system
- Hours saved daily from automated compliance checks and remediation
- Days saved monthly on software updates, such as updating the 9-1-1 computer-aided dispatch application
- Value equal to adding two to three IT staff
- Stronger security posture from dramatically improved device compliance

Why Forescout?

A security analyst on Pontillo's staff had participated in a Proof Of Concept (POC) of the Forescout platform at a previous job. Having seen how the solution agentlessly provided continuous, real-time visibility of all assets on a network, managed Windows devices as well as unmanaged and IoT devices, he suggested that the Miami Police Department strongly consider Forescout to provide device visibility and control. "We did our due diligence—talking to vendors, reviewing analyst reports and so on—but we didn't do a POC; we knew the solution was well established and would fill our visibility gap, and we needed it yesterday," says Pontillo, "so we moved forward."

Business Impact

Real-time, Accurate Visibility and Asset Inventory

Within three days, the Forescout platform was up and running, providing full visibility across the MPD network, reporting all systems without the appropriate antivirus software and providing a detailed, accurate asset inventory. "With the Forescout platform, we could answer the questions we had been asking for years," says Pontillo. "What devices are there? How many of each type? Where are they located? Are they compliant? What is their patch status? What versions of OS or antivirus or other apps are on each device? One of the first things we used it to do was to locate all of the Windows 7 devices so we could communicate with the users of those devices so that we can upgrade their device. It also helped us quickly determine which devices had issues that needed to be addressed right away and which fixes could wait."

Faster, Easier Device Compliance Through Automation

With the Forescout platform, device compliance has improved tremendously, reducing risk exposure across the MPD enterprise. Pontillo and his staff used the Forescout solution to quickly create policies to automate compliance checks, such as ensuring that all mobile devices have full disk encryption and up-to-date antivirus software running. If a device does not have the right version or it's not running, the Forescout platform automatically takes actions to remediate the issue. "For instance, Forescout can tweak the registry, reboot the device and recheck it to verify compliance, or it can force an update or uninstall broken software," explains Pontillo. "If a device still remains noncompliant, then we can quarantine it on a VLAN or display a pop-up window notifying the user to do something."

Hours Saved Daily and Reduced Service Desk Workload

"After the success we had making devices antimalware compliant, it was a no-brainer to use the Forescout platform to update our 9-1-1 computer-aided dispatch software," notes Pontillo. "In the past we would have had to either try to push it out manually or require our computer support team to physically touch hundreds of devices, which is not only time-consuming but increases the probability of human error. Using the Forescout platform, we were able to update 400 to 500 clients in a couple days. Automating remediation has eliminated a lot of work, especially for the computer support team."

> "My team saves hours every day with the Forescout platform. It has become worth two or three IT staff members, helping us to find and resolve device-related issues on a large scale in a very short amount of time."
>
> — Joseph Pontillo, Information Systems Manager, Miami Police Department

Business Value Equivalent of Adding Two to Three IT Staff

"My team saves hours every day with the Forescout platform," adds Pontillo. "It has become worth two or three IT staff members, helping us to find and resolve device-related issues on a large scale in a very short amount of time. With limited staff, time is always scarce, so the efficiency gains we are experiencing from automation are invaluable."

In the future, the Miami Police Department expects to reap additional efficiencies by integrating the Forescout platform with security tools such as McAfee® antimalware protection and Palo Alto Networks® WildFire® cloud-based threat analysis using Forescout eyeExtend products. Pontillo's staff is also in the process of creating dynamic network segmentation policies to automatically quarantine compromised device to specific VLANs and automatically enforce network access control. "In the future, we expect our investment in Forescout to provide even greater value than it already does," concludes Pontillo.

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