Case Study

FORESCOUT

Prince George's County

Forescout Helps Maryland County Identify and Remediate Security Risks While Improving Asset Management and Compliance

THOUSANDS
of unknown devices discovered

$800K
saved annually

RISE
in IT staff efficiencies

Prince George's County MARYLAND

Industry
Public sector

Environment
County-wide network serving approximately 20,000 endpoints, guests, OT and IoT devices

Challenge
- Improve visibility to identify and assess security risk of all devices on the county network, including guest and IoT devices
- Quickly and easily pinpoint unauthorized and noncompliant devices and remotely remediate vulnerabilities
- Shed light on unnecessary assets that increase risks and operational costs
- Help county agencies ensure compliance with federal regulations

Overview

Prince George's County, Maryland, which sits at the eastern border of Washington, D.C., is home to more than 900,000 residents, making it the second most populous county in the state. The county employs approximately 8,000 people spread across 300 different buildings. One of those employees is Jason Arnold, the county's network infrastructure manager. His organization, the Office of Internet Technology (OIT), supports the networking needs for all the different county agencies, including health services, fire, police, U.S. Department of Homeland Security, the courts and others. According to Arnold, the OIT team is tasked with monitoring and managing access for about 20,000 devices. In addition to desktops, laptops, mobile phones and printers, that includes more unusual IoT devices and operational technologies such as:

- Thermostats (HVAC systems)
- Refrigerators for the health department (to monitor and report the temperature of pharmaceuticals)
- Panasonic Toughbooks in police vehicles that are linked to the network
- RFID readers used to inventory and track important court documents to ensure they don't leave the courthouse

Business Challenge

"One of the biggest challenges with the county is that we have different agencies with different IT initiatives and needs. Many times, they put their own devices on the network, and we might not be aware of it, so Forescout has opened our eyes."
— Jason Arnold, Network Infrastructure Manager, Prince George's County, Maryland

Security Solution

- Forescout platform
- Forescout Enterprise Manager
- Forescout eyeExtend for Splunk
- Forescout eyeExtend for VMware AirWatch

Use Cases

- Device visibility
- Asset management
- Device compliance
- Network access control

Results

- Dramatically improves visibility into the number and types of devices on the network, especially previously unknown IoT devices
- Helps IT ensure that noncompliant machines are unable to connect
- Saves time and significantly improves IT efficiency by eliminating the need for technicians to travel to county agency sites to find rogue devices or diagnose problems
- Helps the IT team identify unnecessary, redundant and potentially costly equipment, which they can report to the appropriate county agencies
- Automates incident, IT maintenance and compliance reporting
- Automatically alerts users of outof-date security through push notifications
- Will ultimately help different agencies ensure compliance with federal regulations for their industries
- Provides a platform for automating policy-based segmentation

In 2014, the county's OIT team realized it needed a network access control (NAC) solution that would provide a complete picture of all the devices connected to the network. They knew they had to get a handle on the many different types of devices on the county's internal and guest network. The challenge was figuring out how many endpoints there were, where they were located, identifying which posed risks and finding efficient ways to remediate the issues.

Some of their key concerns involved employees bringing in their own unauthorized devices, such as Mac laptops, wireless routers and gaming machines (like Xbox), and hooking them up to the network. In some cases, different agencies, such as the fire department, would createtheir own homegrown devices in order to introduce new functionality to improve their alerting process.

"The fire department, for example, has a home-grown alerting system that displays lights, sounds spoken-word alerts or sends text messages," says Arnold. The OIT team had to identify these, make sure they weren't causing network issues, and remove them if they violated county security policies.

"When we do a refresh, we give everybody from all the different agencies new laptops, and we need to manage these laptops," Arnold explains. "Some folks have older laptops in a closet that they use whenever they have training or need them for other purposes. There are vulnerabilities. And there is patching. There are all kinds of updates that haven't been pushed to these devices because they are just sitting there, not connected."

> "Forescout opened our eyes. It was like—wait a minute—we have 20,000 devices? We thought we had a fraction of that."
>
> — Jason Arnold, Network Infrastructure Manager, Prince George's County, Maryland

Other county network challenges faced by Arnold and team included:

- Finding less time-consuming ways of identifying security issues and locating compromised/noncompliant devices and then quarantining or removing them
- Cutting costs by locating and eliminating redundant and unnecessary county equipment (such as printers on every desk)
- Finding new ways to help different types of agencies comply with federal regulations for their organizations
- Improving efficiency by moving toward automated device discovery, issue identification and remediation and gathering data to support the move

Why Forescout?

The IT team began looking for a solution that offered outstanding visibility, flexible deployment and the ability to support the county's 300+ agency sites from a central location. It also had to accurately classify a broad range of devices, especially agentless devices, which were just beginning to find their way onto the network. The enterprise architect who had previously occupied Arnold's job understood that network access control (NAC) was becoming critical. Based on its solid reputation in the industry, Forescout was chosen to improve visibility, identify risks and accelerate remediation

- Delivers $798,898 in average annual benefits*
- Enables $403,441 in IT staff efficiencies*

*Calculated by Forescout Business Value ROI Tool

Business Impact

Gaining Visibility into the Number and Types of Devices on the Network

Before Forescout was deployed, Arnold remembers being able to identify only about 16 connected devices (beyond the county's regular network assets). He knew the number had grown significantly but didn't know by how much. After installing Forescout, he was surprised to find just how many outside devices were connected to the county's network. "Forescout opened our eyes. It was like—wait a minute—we have 20,000 devices? We thought we had a fraction of that," he says.

Quickly Identifying Unauthorized Devices

After installation, the Forescout platform immediately began discovering devices that the OIT team had no idea were connected to its network.

"There were users who brought in their own Mac devices, and their own wireless routers, which is a major security risk," he says. Arnold also found a number of "Raspberry Pi" devices—small, inexpensive, credit-card-sized computers with their own operating systems. The fire department alerting systems fell into this category. While Raspberry Pi devices were created to help people learn programming skills, they also can be vulnerable to hacks and other security issues. Arnold points out that a major retail store data breach in 2013 occurred as a result of a network-connected Raspberry Pi device that was hacked.

"We used Forescout to detect a dozen Raspberry Pi devices. They turned out to be legitimate," he remarks, "but it was good to identify them. Now we can keep an eye on them and monitor their behavior."

In terms of unauthorized guest devices, Arnold points to Microsoft Windows XP machines as some of the biggest offenders. When the county deployed Forescout in 2014, it had 1,500 XP devices on the network. "Today, we completely block XP machines from coming on the network," he says. "Those are end-of-life and end-of-support, so whether you are a vendor or a guest, we don't allow you to connect with XP. We will be doing the same thing with Windows 7 devices when that time comes."

Accelerating Help Desk and Incident Response

Prince George's County has also deployed Forescout eyeExtend for Splunk® for security information and event management. "Using Forescout, we're getting more data points on the different devices into Splunk," says Arnold. "With better correlation of endpoint data, we can minimize risk and prioritize response."

The IT team is also using the Forescout the Forescout eyeExtend for VMware® AirWatch for end-to-end management of mobile devices. Together, the Splunk and AirWatch solutions complement the See and Control capabilities of the Forescout platform by providing additional contextual awareness, improving device management and helping the county better control network access.

Currently, 10 OIT employees leverage Forescout technology to improve security and efficiently remediate issues. "My engineers and the service desk use it every day. Service desk personnel can type in a user's name or a host name of a computer and get all the information they need displayed on a dashboard. It works

> "I would have to ask somebody to go out there and look around for the rogue device…But now, Forescout is listening to everything, telling us where it is and its compliance posture, so we don't have to go looking for it."
>
> — Jason Arnold, Network Infrastructure Manager, Prince George's County, Maryland

very well. Security and server teams use Forescout to generate weekly reports on managed devices, noncompliant devices and so on," Arnold explains.

Improving Asset Management

Forescout helps manage assets by identifying equipment the county didn't realize it had and might not need. These devices could be sources of inefficiency and higher costs. "One of the big surprises was printers," says Arnold. We have some agencies that have printers on everybody's desk." Arnold pointed out that the county could cut costs here. "Everyone could use a centralized printer and save on printer ink, paper, maintenance, electricity and more," he notes.

With Forescout providing more insight into these types of equipment edundancies, Arnold now runs reports on the issues and gives them to asset management and county statistics departments to assist in budgeting and planning.

Cutting Costs and Improving Efficiency

Arnold says the ease and speed at which Forescout can help his organization zero in on potential threats and other unknown devices has dramatically reduced the amount of time needed to remediate issues.

"Before Forescout, I would have to ping the device, go through all the different switches and look for the MAC address in all the different address tables on the switches to determine a device's location," he recalls. And many times, Arnold points out, those MAC addresses would turn out to be incorrect.

With the Forescout platform, he says, "I simply type in a user's name, and I will see all the different devices that user has, which switch they are connected to and what building they are in. Then I can actually take some action on it."

According to Arnold, tracking down a rogue device used to take as long as an entire day. First, discovering the issue could require several hours, and then there was the problem of figuring out exactly where it was within the county's 300+ buildings. "I would have to ask somebody to go out there and look around for it or ask somebody if they knew of any devices like that. But now, Forescout is listening to everything, telling us exactly where it is and its compliance posture, so we don't have to go looking for it. I can say to the technician, 'It's in this area in this building on this floor. Go get it,'" says Arnold.

Forescout has also reduced the urgency with which Arnold and team would have to remove rogue devices, because Arnold can now justquarantine or switch block them right from where he is. The technicians can pick up the device when time permits.

"The county is using automation for update management and virus definitions," he adds. "If you are not up to date, Forescout will push a remediation and get you up to date. That works incredibly well."

> "If you are not up to date, Forescout will push a remediation and get you up to date. That works incredibly well."
>
> — Jason Arnold, Network Infrastructure Manager, Prince George's County, Maryland

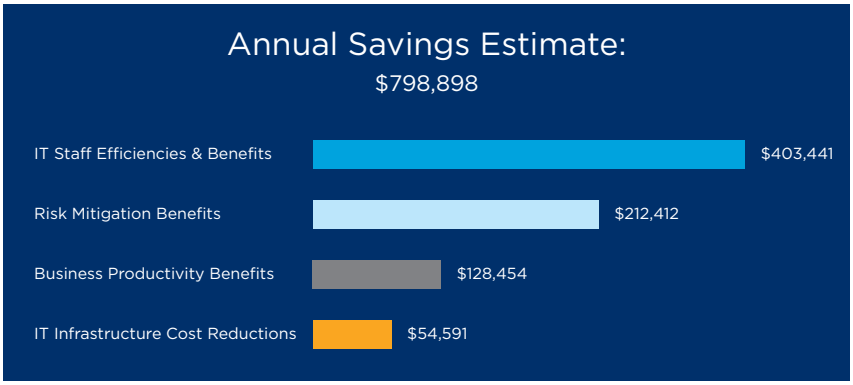
Helping to Ensure Compliance

In addition to complying with network security and other policies, devices for different agencies also need to comply with federal regulations for their industries. For instance, health organizations need to comply with the Health Insurance Portability and Accountability Act (HIPAA) regulations, while financial organizations and other organizations accepting credit cards need to comply with Payment Card Industry (PCI) security standards. Forescout is helping to ensure compliance by automating some of the reports and research the OIT team would previously have to do manually.

Arnold and his team are also looking into network segmentation for the different organizations to help them meet their respective compliance requirements. It plans to segment its network with Palo Alto Networks® Firewalls, and is looking at Forescout eyeExtend for Palo Alto Networks Next Generation Firewalls to simplify integration and segmentation enforcement.

Business Value

Translated into business value, Forescout's Return on Investment Calculator indicates that Prince George's County will realize substantial cost savings in multiple areas. Annual savings are estimated at $798,898, broken down as follows:



Over a period of five years, Prince George's County will likely save as much as $3,994,491.

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 03_20