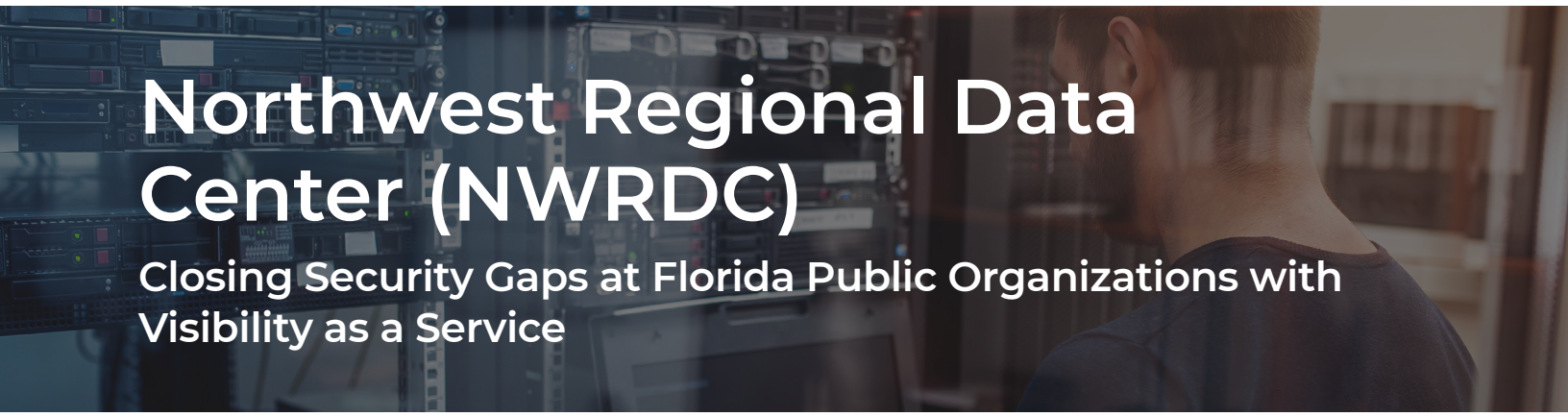
Case Study

FORESCOUT



Northwest Regional Data Center (NWRDC)

Closing Security Gaps at Florida Public Organizations with Visibility as a Service

ROI
found to be much greater than other tools

1,000+
more devices discovered than expected

HIPPA
and other regulations are in compliance

NWRDC™
Northwest Regional Data Center

Industry
Government/Education

Environment
Wireless and wired endpoints at up to 120 public-sector entities, from city governments and state agencies to K-12 schools and universities

Challenge

- Provide increased visibility, NAC, endpoint compliance, improved asset management and faster incident response for a wide range of customers in the public sector
- Make comprehensive visibility across the network easy to obtain and more affordable

Security Solution

- Forescout platform
- Enterprise Manager

Overview

Based in Tallahassee, Florida, the public Northwest Regional Data Center (NWRDC) is the state of Florida's primary provider of computing services, serving 120 public-sector entities in the state, from small city governments and K-12 school districts to higher education institutions and state-level agencies that serve every Florida citizen. An auxiliary of Florida State University, NWRDC provides cost-effective services and support that enable these entities to respond to disasters, ensure uptime, provide business continuity and defend against cyberattacks. As executive director, Tim Brown oversees technological innovation, customer service, fiscal management, and developing partnerships with IT vendors and service providers. In recent years, he and NWRDC Chief Technology Officer Matt Stolk have directed the gradual transformation of the Center to a full-service provider via the cloud, providing services that many organizations could not obtain on their own. Although their reasons vary, most NWRDC customers share the need to better understand what is on their networks at any given time. Consequently, Brown and Stolk championed the introduction of the Center's latest offering: Visibility as a Service (VaaS). In the process, they learned that the service, developed in partnership with Forescout Technologies, could deliver much more than just visibility.

Business Challenge

"You can't secure what you can't see. The reasons vary across organizations, but all can benefit from more comprehensive visibility across their networks."
— Tim Brown, Executive Director, Northwest Regional Data Center

In 2016, risk assessments of multiple public-sector entities in Florida all highlighted the need for better visibility across their networks. "In today's ever-changing cyber climate, seeing exactly what and who is accessing or trying to access your network is essential to having confidence in your security posture," says Stolk. "The state security assessments showed or confirmed that some

Use Cases

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

Results

- Provides comprehensive visibility across networks, improving data center security posture
- Facilitates compliance with FERPA, HIPAA, PCI, NIST, and numerous other regulations
- Saves money and enables procurement as an operating expense rather than a capital expense
- Enhances asset management and automates discovery and notification of devices as soon as they appear on the network
- Provides capability to integrate directly with other security solutions, enabling bidirectional automation, improved protection and greater operational efficiencies

> "With Forescout and Visibility as a Service, you can check the box on many different pain points in an organization all at the same time."
>
> — Tim Brown, Executive Director, Northwest Regional Data Center

organizations needed better network access control, others a way to integrate NAC into their configuration management database (CMDB), and still others improved endpoint compliance for FERPA, HIPAA, CJIS, PCI or any number of other regulations."

Why Forescout?

Greater Reach and Return on Investment

"We looked at a number of security tools that addressed various issues— for instance, NAC-specific tools and configuration management database plug-ins—but each only addressed one niche area and couldn't help all of our customers," notes Stolk. Then NWRDC discovered Forescout.

"When I first saw the Forescout solution, I was underwhelmed," Stolk admits. "I thought, 'We've already got products that do these things.' But the more I looked into it, the more I realized that our products stop at one level and Forescout picks up where they stop and carries them to the next level. It also allows separate tools to integrate and share data and insight. Visibility as a Service is such a simple term, but the solution does a whole lot more than just find devices on your network."

"We realized that Forescout could meet multiple visibility needs across the state, well beyond just NAC," continues Stolk. "It was also more costeffective than many point solutions, such as the licensing for the CMDB plug-in, which only integrated with the one ITSM tool. In short, Forescout provided much better bang for the buck."

Consequently NWRDC decided to partner with Forescout Technologies to provide its technology to the Center's customers via a subscriptionbased Visibility as a Service. Using an agentless approach, VaaS provides rapid visibility across all devices as they connect to a network, whether via wired, wireless or VPN connection. The service automatically determines the user, owner, operating system, device configuration, software, services, patch state and the presence of security agents for all devices—while providing continuous remediation, control and monitoring of these devices.

Business Impact

Discovering Thousands More Devices than Expected

Most of the Florida public organizations using NWRDC's Visibility as a Service have discovered almost immediately that they have many more devices on their networks than they realized. "The devices that VaaS discovered ranged from forgotten, obsolete workstations to unauthorized smartphones and much more," recalls Brown. "With VaaS, these organizations now have at their fingertips all the pertinent details to locate and manage these devices. Asset management is one of the most critical security controls for any organization."

Making Visibility Affordable

"Every NWRDC customer desires a strong security posture and most know what they need to do to achieve it, but budgetary constraints and legislative hurdles often cripple them," explains Brown. "For many, the ability to gain comprehensive visibility without having to spend the money on expensive hardware and added operational overhead— to use Opex rather than or in conjunction with Capex funds—makes procurement possible."

> "We realized that Forescout could meet multiple visibility needs across the state, well beyond just NAC. It was also more cost-effective than many point solutions…In short, Forescout provided much better bang for the buck."
>
> — Matt Stolk, Chief Technology Officer, Northwest Regional Data Center

In addition, organizations using VaaS reap significant cost savings passed on by NWRDC. (The Center negotiates significant discounts with all its partners.) NWRDC's status as an auxiliary of FSU allows public entities to contract directly with it without engaging in a lengthy procurement bid process.

Furthermore, NWRDC customers save because they don't have to maintain or refresh any hardware. Since the Forescout solution does not require the installation of software agents, implementation is easy. Within just a few days, the organization has complete visibility of all devices connected to the network at the moment they connect, with context around their posture and compliance.

Benefitting Internally from Improved Asset Management

Internally, NWRDC is also benefitting from the new service. "We saw a need to improve our manual asset inventory processes, and wanted to automate steps in the discovery and notification of new devices on our network," explains Stolk. "The Forescout solution helped us do just that. In addition to supplying us with an accurate asset inventory, it lets us know exactly what is plugged into our network and what devices are available at any given moment."

Flexibility to Fill Multiple Security Gaps and Meet a Broad Range of Use Cases

As noted, one of NWRDC's customers uses the VaaS service as a discovery tool to streamline its security incident management efforts and to populate its CMDB. Another uses it to continually hunt for any network vulnerabilities and unforeseen network intrusions. Others have switched from reactive to proactive network scanning because it is now so easy to scan the network for abnormalities. The NWRDC itself is deploying Forescout Extended Modules to automate tasks and enhance the capabilities of its existing vulnerability management, firewall, and endpoint compliance solutions.

"With Forescout and Visibility as a Service, you can check the box on many different pain points in an organization all at the same time," says Brown. Take, for example, the NWRDC customer with a team tasked with accurately populating its CMDB. After learning more about VaaS, the team realized it could be used to solve five or six other security-related issues in its organization.

When talking with prospective customers about signing up for VaaS, Stolk shares some advice, which applies to others who may be considering Forescout as well: "When you first start looking at the Forescout solution, make sure you understand its breadth and reach before you discount it; it does things in a much different way than your existing tools, at a much different level of detail. And it has the flexibility to fit a wide range of use cases and fill numerous security gaps."

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