Case Study

TDOT

Tennessee Department of Transportation Counts on Forescout to “Guard the Guards” and Reduce Risk of Business Disruption or Breach

95%
of devices auto-classified

27 HOURS
time savings per week

$500K
in annual savings from reduced insurance premiums

Industry

Transportation, Government

Environment

5,000 wired and wireless endpoints statewide, including IT, IoT and OT and devices in remote, campus, cloud and data center environments

Challenge

- Reduce risk of business disruption from security incidents or breaches
- Continuously ensure and demonstrate security compliance across all devices connected to the network
- Drive security operations efficiencies and efficacy through integration and automation

Overview

The Tennessee Department of Transportation (TDOT) serves the transportation needs of the state’s 5.7 million residents across the state’s 14,000 miles of roadway as well as railways, waterways and 80 airports. To reduce the risk of network disruption or a security breach, TDOT’s cybersecurity staff wanted absolute visibility of all devices—including IoT and OT devices, virtual machines and network infrastructure—so it could validate the integrity of data generated by its other security tools. With the Forescout device visibility and control platform, TDOT gained comprehensive, real-time visibility across all the enterprise’s endpoints and a “source of truth” to check the trustworthiness of information generated by other security systems in its environment. The Forescout solution addresses additional use cases at TDOT as well; for instance, from its first hour in production, it began helping to improve device compliance. Since then it has also resulted in significant, measurable time and cost savings.

Business Challenge

“If one of our key security tools is compromised and starts giving us dishonest information, how will we know?”
— Richard White, Cybersecurity Architect, Tennessee Department of Transportation

Strategic Technology Solutions (STS), the State of Tennessee department that runs and controls information technology for the state’s government operations, runs TDOT’s switches and routers and controls some of its Active Directory and other security controls. Consequently, the TDOT cybersecurity team lacks access to things like switch management for discovery purposes. They could direct a switched port analyzer (SPAN) at their security tools to monitor traffic but they had no way to validate patches or other compliance-related information on devices without requesting a report from STS.

“We have a lot of great security tools protecting our endpoints—but we needed a way to obtain visibility across devices without going through STS,” explains TDOT Cybersecurity Architect Richard White. “We also desired a way to make sure the tools are being honest, that they haven’t been unknowingly compromised.”

Why Forescout?

Comprehensive Visibility Proves Business Value in Less than an Hour

When the TDOT cybersecurity team learned that the Forescout device visibility and control platform provides agentless device discovery and classification in real time plus continuous posture assessment, they decided to test it in a two-week proof of concept using live data. “The quality and breadth of data the Forescout platform provided and all the use cases it could address, from device compliance and detection of rogue devices to asset management and incident response, impressed us all,” recounts White. “Plus, we would no longer have to wait on other people to gain visibility or control.”

The team was also amazed at how quickly the Forescout platform began proving its worth. “We plugged in the Forescout appliance, and in less than an hour it was fully operational, and we were collecting valuable data that would help mitigate compliance risks and validate other sources,” White continues. “In every aspect, deployment was quick and easy. For instance, in less than two hours we were monitoring Voice over IP at all of our traffic management centers.”

Business Impact

Discovered Noncompliant Devices that Other Security Tools Missed

“We have Cisco Identity Services Engine (ISE), network traffic analyzers, AI-based behavioral analysis software and other security products—but the Forescout platform found everything on our network better than any of them,” claims White. “For instance, it detected a computer still running Microsoft XP that neither Active Directory nor any of our other tools caught. It also gave us highly granular information and produced the best asset inventory we’ve ever had.”

“Forescout gives us the critical integrity piece of the ‘CIA triad’—confidentiality, integrity, and availability,” adds White. “Without integrity, the other two are of no value. You need to be able to trust your systems when they tell you your data is confidential and available. The Forescout platform lets us know whether their data can be trusted.”

Improved Device Compliance with Real-Time Posture Assessment and Classification

In addition to the PC running XP, the Forescout platform’s real-time device posture assessment uncovered workstations that needed patching or upgrading, devices with Telnet turned on that they had thought had been turned off, legacy machines without strong password capability, and other at-risk, noncompliant devices. In total, it found 10 to 15 percent of all devices lacked compliance to some degree—which TDOT staff immediately addressed.

To aide with compliance, TDOT also uses the Forescout platform to automatically classify and categorize more than 95 percent of its devices. For instance, classification by the street zone segment in which the device is located enables

Security Solution

- Forescout platform
- Forescout eyeExtend for Symantec Endpoint Protection
- Forescout eyeExtend for Splunk

Use Cases

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

Results

- Reduced risk of business disruption from a security incident or breach
- Business value evidenced within one hour
- Auto-classified and categorized over 95 percent of devices out of the box
- Rapid discovery and remediation of the 10-15 percent of total devices found to be non-compliant
- Continuous assessment of devices as they connect to the network to enforce compliance policies
- Time savings of 27 hours per week (more than two-thirds of one full-time employee)
- Cost savings of $300,000 to $500,000 annually from reduced insurance premiums
- Automated incident response actions thanks to integration with Splunk SIEM
- Accurate asset inventory across IT and OT networks, including agentless devices
- A robust, truly multi-layered cyberdefense to provide confidentiality, integrity and availability

application of the strictest security policies to devices within critical infrastructure zones.

> "Forescout gives us the critical integrity piece of the CIA triad. Without integrity, the other two are of no value. You need to be able to trust your systems when they tell you your data is confidential and available. The Forescout platform lets us know whether their data can be trusted."
>
> — Richard White, Cybersecurity Architect, Tennessee Department of Transportation

Saving 27 Hours Each Week Through Centralized Visibility and Automation

By automating and streamlining manual activities, the Forescout platform saves the TDOT cybersecurity team approximately 27 hours each week—more than twothirds of a full-time employee. "To find information about devices on the network, we no longer have to sit and wait for a ping sweep or go to four or five different systems and pull log files," White explains. "We now have one central place to answer all our visibility-related questions—what IP addresses are currently active, where a specific device resides, where all the devices of a given type are, how many there are, when they were last logged into, which version of an application they are running, which devices need updating, which were affected by an incident, and so on—all without requiring agents or writing scripts. The Forescout platform really is a one-stop shop for visibility."

Saving $300,000 to $500,000 Annually in Insurance Premiums

Thanks to the Federal Information Securities Modernization Act, U.S. government entities can submit an incident response plan to receive a discount on the liability insurance premiums it pays to cover the financial impact of a breach. TDOT submitted a plan featuring the Forescout platform as a key component. "Our incident response plan saves us between $300,000 and $500,000 each year in discounts—or between $900,000 and $1.5 million in three years," notes White.

Orchestration to Help Automate Incident Response and Bolster OT Defenses

TDOT has also been piloting and plans to implement Forescout eyeExtend for Splunk to integrate the Forescout platform with its SIEM. The Forescout platform discovers infected devices and sends the information to the SIEM, which then automatically initiates policy-based mitigation actions to contain and respond to the event. For instance, it can alert users, initiate scans by another security tool and share real-time context with other incident response systems to accelerate quarantining or other remediation.

The TDOT Cyber Security plan is standing-up a Cyber Security Protection team (Flat-Earth) to monitor the Active Intelligent Traffic Network (Active-ITS) 24/7. Extending the Forescout platform and integrating with Splunk, the Computer Protection team will have additional tools to analyze zero-day events. TDOT's Active ITS network is a critical infrastructure serving drivers throughout the State of Tennessee. Information must be accurate and have the integrity to ensure travelers make a safe destination while travelling on Tennessee highways.

In addition, TDOT plans to use other Forescout eyeExtend products to gain workflow interoperability with other security tools, enhancing their effectiveness by providing greater situational awareness. "Our goal is to have the Forescout platform, Cisco ISE and other security solutions all working together to watch one another and keep us safe," says White.

TDOT is also currently evaluating Forescout SilentDefense™. "Forescout SilentDefense is the most advanced and mature OT network monitoring and intelligence platform available," explains White. "We want to use it to automatically learn and validate network communication patterns, and to apply the most in-depth analysis of industrial protocols to create network and protocol whitelists."

TDOT's success with Forescout has other departments within the Tennessee government considering the Forescout platform too. "Buying the Forescout platform is the best first step for improving device compliance and reducing the risk of a security incident or breach," states White.

> "We have Cisco Identity Services Engine (ISE), network traffic analyzers, AI-based behavioral analysis software and other security products—but the Forescout platform found everything on our network better than any of them. For instance, it detected a computer still running Microsoft XP that neither Active Directory nor any of our other tools caught. It also gave us highly granular information and produced the best asset inventory we've ever had."
>
> — Richard White, Cybersecurity Architect, Tennessee Department of Transportation

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