Case Study

FORESCOUT
Active Defense for the Enterprise of Things™

# U.S. State Government Agency

## State Agency Saves 13 Hours Weekly with Forescout Platform

**3 DAYS**
to achieve enterprise visibility

**13 HOURS**
saved weekly on device compliance

**WEEKS**
saved identifying and remediating vulnerabilities

**Industry**
Government

**Environment**
10,000 wired and wireless devices across multiple divisions and 220 sites; 4,200 employees

**Challenge**

- Provide business continuity to deliver a wide variety of public services
- Safeguard PPI and other sensitive information
- Minimize security risk by keeping devices compliant and blocking noncompliant devices from accessing the network
- Comply with state and federal regulations while reducing time spent on operational audits

## Overview

This U.S. state government agency works to protect its environment, safeguard consumers and ensure food safety. Its programs and activities are so varied and extensive they touch almost every state resident. By implementing the Forescout platform, the organization addressed security, compliance and network access gaps to dramatically improve its overall security posture. Also, its information security and networking teams save multiple days each month, accelerate incident response, improve governance and streamline their transition to Zero Trust.

## Business Challenge

*"To know what was on the network, and the compliance state of each connected thing took tremendous time and effort and hindered our ability to implement NAC."*
— Chief Technology Officer, U.S. State Government Agency

The agency's Chief Technology Officer (CTO) oversees the technology needs of 220 sites across multiple, extremely diverse divisions spread across the state. His immediate priority was to address the results of an external state cybersecurity assessment. The audit highlighted significant security gaps in device visibility and compliance across the organization's network and the need for network access control (NAC). "We couldn't trust that each site's devices were compliant or that we were seeing everything on the network," he recalls. "Manually verifying and remediating all 10,000 endpoints just wasn't an option because it was too time-consuming and error-prone."

### Security Solution

- Forescout platform
- Forescout eyeSegment
- Forescout eyeExtend for McAfee® ePO™

### Use Cases

- Network access control
- IoT security
- Network segmentation
- Incident response
- Asset inventory
- Device compliance
- Regulatory compliance
- Security orchestration

### Results

- Visibility across every connected thing within three days after implementation
- Discovered 10% more devices on the network than expected
- 13 hours saved per week on device hygiene and compliance
- 8 days saved tracking down Windows 7 devices
- 5 to 7 days saved addressing Windows Zero-Day vulnerabilities due to Forescout policy templates
- Minimized risk thanks to continuous monitoring and posture assessment
- Streamlined regulatory compliance and reporting due to comprehensive visibility of devices and traffic patterns
- Improved situational awareness and faster time to incident identification and remediation
- Noncompliant and rogue devices blocked from accessing network
- Accelerates transition to Zero Trust network
- Accurate, real-time asset inventory alleviated the need for $42,000 asset management tool

## Why Forescout?

When the CTO joined the agency, the information security team had already conducted a Proof of Concept (POC) of the Forescout platform. The solution's agentless approach and rapid time to value had made the information security manager a strong advocate. The CTO himself had also been impressed by a Forescout POC while working at a different agency within the state. He also appreciated that, unlike the alternative solution, implementing the Forescout platform would not require upgrading any network infrastructure. "From a visibility, compliance or efficiency perspective, the competition simply could not come close to Forescout," he says. "And for the overall value it gives us, it was well worth the investment."

## Business Impact

### Real-Time Source of Truth for All Devices on the Network

The agency's IT staff thought there were 9,700 networked devices, but within just three days, the POC uncovered 10,200 systems – 10% more than expected. The Forescout platform also automatically classified all the devices, including the organization's 3,000 IP phones. "In both my previous agency and this one, unlike other tools, the Forescout platform has always provided 100% accurate visibility," says the CTO. "We now have confidence that we know exactly what is on our network at any given time."

### Faster, Easier Device Compliance and Audit Reporting

With the Forescout platform continuously monitoring and assessing the security posture of endpoints, the CTO and his staff no longer have to wonder if the device compliance reports from the various divisions and sites are accurate. They can instantly view the compliance status of every network-connected thing at any time. Providing reports for auditors – a task that previously took a minimum of several hours – now takes just minutes, even for business executives and other non-technical personnel. "It's also easy to locate noncompliant devices and isolate them," notes the CTO. "We saved eight workdays just tracking down and remediating end-user machines."

### Time Savings from Automation

Since implementing the Forescout platform, the state agency's IT, security and networking teams save approximately 13 hours of work every week. For instance, by integrating the Forescout solution with the organization's McAfee® antimalware software, they have automated antivirus updates and most remediation activity. If updates are not successful the first time, the Forescout platform can automatically take steps to remediate, such as tweaking the registry, rebooting and rechecking the device to verify compliance, forcing updates or uninstalling broken software. In the future, integrating the Forescout platform with other security tools will increase time savings even more.

### Additional Time and Cost Savings

The CTO also cites the responsiveness of both Forescout support and advanced research teams as huge time savers. "Within a day of the MS-ISAC announcing the Windows Zero-Day vulnerability, Forescout released a policy template to check for vulnerable endpoints," he says. "With the template, we immediately identified our endpoints that were vulnerable and began remediating them,

> "When there is trust, there is speed. The Forescout platform is invaluable because it provides the level of visibility that gives us that trust—trust that we know exactly what devices are on our network, along with the situational awareness both to be proactive and to address issues as they arise."
>
> — Chief Technology Officer, U.S. State Government Agency

saving us five to seven days of research and protecting our network that much faster." In addition, because the Forescout platform provided a detailed, real-time asset inventory, the organization canceled plans to purchase asset management software, saving over $40,000 and time spent learning a new tool.

## Fortifying Security and Minimizing Risk with NAC and eyeSegment

With comprehensive visibility now in hand, the CTO and his staff are focusing on NAC and using the Forescout platform to block all noncompliant devices and direct devices to specific VLANs. After a suspicious rise in users being locked out of their accounts, the team implemented Forescout eyeSegment. "With eyeSegment, we see anomalies in traffic patterns and behaviors almost instantaneously," says the CTO. "Within hours of implementing eyeSegment, we pinpointed the attack point of entry and began to remediate."

Using eyeSegment has led security and network teams to make important policy, procedural and configuration changes and is accelerating the agency's journey to Zero Trust. "With the level of visibility and control we have gained and the myriad ways we save time and close security gaps, the Forescout platform has proved invaluable," states the CTO. "In addition, Forescout's customer service is elite and very proactive. For me, having a trusted partner outweighs almost everything."

FORESCOUT
Active Defense for the Enterprise of Things™

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