Case Study

FORESCOUT
Active Defense for the Enterprise of Things™

U.S. State Government Agency

U.S. State Government Agency Saves More Than Eight Days Each Month with Forescout Platform

3 DAYS
to achieve enterprise visibility

10+ HOURS
weekly saved on device compliance

5+ DAYS
saved responding to Windows Zero-Day announcement

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 services to the public
- 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

Security Solution

- Forescout platform
- Forescout eyeExtend for McAfee® ePO™

Overview

This U.S. state government agency works to protect its state's environment, safeguard its consumers and ensure food safety. Its programs and activities are so varied and extensive, they touch almost everyone in the state. By implementing the Forescout platform to obtain accurate, granular device visibility and continuous posture assessment, the organization addressed security, compliance and network access gaps to dramatically improve its overall security posture. The organization's information security and networking teams also save more than eight days each month thanks to automated compliance and remediation tasks, easier audit reporting and policy templates proactively provided by Forescout.

Business Challenge

"To find out what was on the network or whether antivirus protection or patching was current and working took a tremendous amount of time and effort."
— Chief Technology Officer for a U.S. State Government Agency

The Chief Technology Officer (CTO) of this U.S. state agency oversees the technology needs of 220 sites across multiple, very diverse divisions spread across the state. When he became CTO, one of his immediate priorities was to address the results of an external state cybersecurity assessment. The audit had found 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. "And manually verifying and remediating all 10,000 endpoints just wasn't an option because it took way too much time and was too error-prone."

Use Cases

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

Results

- Visibility across enterprise within three days after implementation
- Discovery of 10% more devices on the network than expected
- 10 to 14 hours saved per week on device hygiene and compliance
- 8 days saved tracking down Windows 7 devices
- 5 to 7 days saved researching and creating policy for Windows Zero-Day vulnerabilities due to policy templates provided by Forescout
- Minimized risk thanks to continuous monitoring and posture assessment
- Faster, easier regulatory compliance due to comprehensive visibility and ease of reporting
- Improved situational awareness and faster time to remediation
- Noncompliant and rogue devices blocked from accessing network
- Accurate device visibility resulting in greater confidence and peace of mind
- Accurate, real-time asset inventory alleviated 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 for device visibility and network access control. 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. Furthermore, he 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 claims. "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 devices on the network, but within just three days the Forescout POC uncovered 10,200 devices—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—for instance, checking on the status of antivirus definitions and patch updates—the CTO and his staff no longer have to wonder if the device compliance reports from the various divisions and sites are accurate. Using the Forescout dashboard, they can instantly view the compliance status of devices on the network at any given time. Printing reports for internal and external auditors, a task that in the past could easily take a minimum of several hours now takes just minutes, even for business executives and other non-technical personnel. "Satisfying auditors is so much easier now," claims the CTO. "It's also easy to locate noncompliant devices and isolate them. We saved around 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 10 to 14 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.

"When there is trust, there is speed. Without trust, everything bogs down. 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 for a U.S. State Government Agency

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, 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 cancelled plans to purchase asset management software, saving over $40,000 and time spent learning a new tool.

Fortifying Security and Minimizing Risk with NAC

To further reduce risk of business disruption or access to sensitive data, the CTO and his staff are also beginning to expand and enhance their use of the Forescout platform for NAC. For instance, they are currently planning to test automatic blocking of managed devices that lack up-to-date McAfee endpoint protection when they try to connect to the network. (Users are notified via pop-up window to update the software and try again.) They also plan to enable devices to be dynamically directed to specific VLANs upon connection to the network —such as automatically restricting legacy scientific equipment to their own VLAN.

"With the level of visibility 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. Together we have built a terrific partnership."

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