



State of Missouri

Visibility. Integration. Automation. ForeScout
Makes A Strong Showing in the Show-Me State

10,000

additional endpoint
devices discovered

INSTANT

detection from FireEye
allows ForeScout to
quarantine the device

HOURS

to deploy with full
visibility



Industry

Government

Environment

40,000 employees/devices
distributed across 100+ locations

Challenge

- Improve visibility and control of endpoints—especially unmanaged endpoints
- Accelerate threat response
- Automate multisystem interoperability

Security Solution

- ForeScout platform
- Enterprise Manager
- ForeScout eyeExtend for EMM
- ForeScout eyeExtend for ATD

Overview

The Center for Digital Government lists Missouri among the leading states for implementing information technology to serve its citizens. The state's Information Technology Services Division supports 14 state agencies and roughly 40,000 employees distributed across more than one hundred state offices.

Business Challenge

Given the increased importance of cybersecurity and security compliance, Missouri State Chief Information Security Officer Michael Roling posed this question to his staff: "Exactly what devices are on our network, and are they all secure?" As Roling suspected, this was a difficult question to answer. After conducting a compliance audit in 2012, it became clear that Missouri had limited visibility into what was on its networks. "We already knew we had visibility issues with unmanaged and BYOD devices," said CISO Roling. "So, the compliance finding helped us obtain funding to address the issue."

Why ForeScout?

After briefly considering a competing solution from a major in-house vendor, Roling and his team determined the 802.1X platform lacked the maturity and documentation to meet the requirements of his organization. Roling began researching alternatives and discovered ForeScout in the Gartner Magic Quadrant* for Network Access Control. "ForeScout ranked very highly in the Gartner report," stated

Roling. "At the time, I'd never heard of the company, so I started making a few calls." Roling and his team decided to put the ForeScout platform through its paces

Use Cases

- Device visibility
- Device compliance
- Network access control
- Incident response

Results

- Deployed the Forescout platform appliance within hours
- Gained instant visibility of previously unknown devices
- Deployed policy-based access controls in days
- FireEye integration through Forescout's eyeExtend for ATD allows automated quarantine and control of infected endpoints
- MobileIron Integration through Forescout's eyeExtend for EMM allows automated mobile device management access control
- Maintained flexibility to switch enterprise mobility management platforms on the fly
- Gained centralized management of network access control for 100+ sites and 40,000 plus users
- Quickly discovered and mitigated unknown Windows XP endpoints when Microsoft ended XP OS support

in a proof-of-concept evaluation. "We were told we could deploy the Forescout platform in an afternoon," said Roling. "I looked at one of my team members and we both rolled our eyes. Then we actually deployed it in a few hours!" With the Forescout platform up and running, Missouri's IT Services Division team instantly gained visibility into networked devices that had previously been invisible.

In addition, they benefited from something Forescout doesn't do: Vendor lock-in. "Our strategy employs a best-of-breed approach that must embrace many types of technologies and vendors, and Forescout fit in perfectly," Roling said. "Once we saw the openness of the Forescout platform, we knew we had picked the right one," he added.

Business Impact

Network Visibility is Enlightening

CISO Roling spoke at length about his team's pre-Forescout assumptions as well as discoveries once the platform was in place:

"I really didn't have any idea of how many devices were on our network. We thought it was in the neighborhood of 30,000 devices at any given moment. Buried in these numbers are the machines we didn't know about. We found a lot of industrial control systems, HVAC, building automation systems—a lot of devices with embedded OSs. We also detected a number of devices that did not meet our compliance policies—devices running out-of-date OSs that weren't manageable, as well as some personal devices that shouldn't have been on our network. It's that handful that you need to be concerned about. Forescout gave us visibility into those machines that we needed to take action on."

Policy Creation Ensures Endpoint Compliance

Once Forescout unveils what's on your network, you can build policies that target the devices that put your network at risk. One example of this occurred in April 2014, when Microsoft ended support of its Windows® XP operating system. The State of Missouri devised a policy that the Forescout platform acted on to find and mitigate all Windows XP-based PCs and laptops on the network, including those that could avoid detection by other solutions because they only logged on sporadically. Through continuous, policybased detection, Roling and his security team quickly identified all XP-based machines and notified the desktop and end-user management teams who were then able to remediate them—either by retiring, replacing or upgrading.

Flexibility Through Integration

One of the primary benefits of Forescout technology is integration with other network security products via orchestration capabilities. Roling is enthusiastic about Forescout integration—not only as it relates to immediate security automation and efficiency, but also because of the flexibility it provides.

Flexibility in Advanced Threat Detection: "We leveraged the Forescout eyeExtend for Advanced Threat Detection with FireEye. When FireEye detects an infected host, it instantly informs the Forescout platform which quarantines the device and begins policy-based mitigation actions. When my staff sees a FireEye event and they are in the middle of doing another activity or away from the office, they know that Forescout will contain the attack—and that is tremendous. That single

“When it’s late at night, or when my staff is sleeping, the Forescout platform is working with our other security solutions to take immediate action on threats. You can’t put a price tag on that type of automation.”

— Michael Roling, Chief
Information Security Officer, State
of Missouri

purchase has greatly enhanced my staff’s lives in terms of responding to incidents. It reduced the time we spend on threat response, allowing us to use that time delivering greater value.”

Flexibility in Enterprise Mobility Management: “We were a MobileIron® shop and used Forescout eyeExtend for EMM to plug the Forescout platform into MobileIron. Now we’re transitioning to AirWatch®. The same module works for both. Having the same access control solution in place and leveraging very different and competitive EMM platforms is a huge win for my team.”

Moving forward, Roling isn’t certain how cybersecurity will play out in the years ahead. He is certain about one thing, however. “Security is all about process improvement. Networks evolve and security solutions evolve. As we acquire new solutions, I’m very confident that Forescout will be right there with us to leverage those technologies and automate processes.”