carahsoft

FORESCOUT

Forescout Makes A Strong Showing for Public Sector Cyber Leader

Visibility. Integration. Automation.

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA, NASA SEWP V, ITES-SW2 and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Forescout, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/ForescoutResources

Join Events & Webinars:
carah.io/ForescoutEvents

Discover Technology Solutions:
carah.io/Forescout

Learn About Procurement:
carah.io/ForescoutContracts

Connect With Our Team:
Forescout@carahsoft.com
(833) FSCT-GOV

FORESCOUT

CASE STUDY

carahsoft

Visibility. Integration. Automation.

Forescout Makes A Strong Showing for Public Sector Cyber Leader

State & Local Government

Business Challenge

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

Why Forescout?

After briefly considering a competing solution from a toolset they already owned, the CISO and his team determined their existing toolset lacked the maturity and documentation to meet the requirements of his organization.

He began researching alternatives and discovered Forescout. "At the time, I'd never heard of the company, so I started making a few calls," said the CISO. He and his team decided to put the Forescout platform through its paces in a proof-of-concept evaluation. "We were told we could deploy the Forescout platform in an afternoon," said the CISO. "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, the state's IT Services Division team instantly gained visibility into networked devices that were previously 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. Once we saw the openness of the Forescout platform, we knew we had picked the right one."

Business Impact

Network Visibility is Enlightening

The CISO 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 discovered 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 surfaces what's on the network, security operations staff can build policies that target the devices that put the network at risk. One example of this occurred when Microsoft ended support for one of its operating systems (OS.) The team devised a policy that the Forescout platform enforced to find and mitigate all PCs and laptops with that OS and were connected to the network, including those that could avoid detection by other solutions because they logged on sporadically.

Then, through continuous, policy-based discovery, the CISO and his security team quickly identified all the machines with the end of life OS and notified the desktop and enduser management teams who were then able to remediate them—either by retiring, replacing or upgrading.

Flexibility Through Integration

One of the primary benefits of the Forescout technology is integration with other network security products via orchestration capabilities. The CISO was 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 Ecosystem for advanced threat detection. When an infected host was discovered, it instantly informed the Forescout platform which quarantined the device and began policy-based mitigation actions. Now, when my staff sees an event and they are in the middle of another activity or away from the office, they know that Forescout will contain the attack—and that is tremendous. That single purchase has greatly enhanced my staff's lives in terms of responding to incidents. It reduced the time we spend on threat response and allows us to use that time delivering greater value."

Flexibility in Enterprise Mobility Management

"We used the Forescout Ecosystem to plug the Forescout platform into an enterprise mobility management tool. Now we're transitioning to a different EMM tool. Forescout 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, the CISO 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."

"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."

10,000
additional endpoint devices discovered

INSTANT
discovery from integrated EMM 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 IT, IoT, and OT endpoints
- Accelerate threat response
- Automate multisystem interoperability

Security Solution
- Forescout platform
- Forescout Ecosystem and supporting modules

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
- Forescout's Ecosystem integration allowed automated quarantine and control of infected endpoints and automated mobile device management access control
- Maintained flexibility to switch EMM platforms on the fly
- Gained centralized management of network access control for 100+ sites and 40,000+ users
- Quickly discovered and mitigated Microsoft endpoints after Microsoft ended OS support for those endpoints.