Case Study

FORESCOUT

State of Utah

Dramatically Improves Visibility and Control and Projects Huge Compliance Cost Savings

48%
were vulnerable to WannaCry

$1M
Saved from faster audits

SECONDS
rather than hours for incident response detection

Industry
Government

Environment
60,000+ devices across a wired and wireless campus and data center that includes 25 state agencies

Challenge
- Uncertainty as to what is on the network hindered security and asset management
- Lack of clarity on configurations and software agents on devices enabled potential vulnerabilities
- Costly, time-consuming audits drained resources and provided inadequate results

Overview

The State of Utah Department of Technology Services (DTS) provides a wide range of services—cybersecurity, desktop support, telecom, networking, storage, web hosting and more—that span approximately 60,000 endpoints in more than 25 state agencies that serve Utah's 3.1 million residents. The agencies manage the gamut of sensitive data—data governed by as IRS-1075, HIPAA, PCI, CJIS and other regulations.

In 2012, Utah experienced a data breach that cost the state more than $9 million in audits and upgrades. Time-consuming audits continued to drain resources and show security gaps. While starting work on a port authentication solution and network segmentation capabilities in house, Utah DTS discovered the Forescout platform, which provides agentless visibility across the entire network without requiring the DTS to "rip and replace" any hardware or software. The more the DTS officials learned from testing the Forescout solution, they realized that the solution would extend far beyond the state's immediate regulatory compliance, Network Access Control (NAC) and network segmentation needs. In addition, it would save the state a lot of time, hassle and money

Business Challenge

"You have to be compliant; it's not a choice. For a network the size of ours, the man-hours to do so manually cost well over $1 million, and the cost of a breach can go through the roof."
— Phil Bates, Chief Information Security Officer, State of Utah

For years following the 2012 data breach, in which hackers broke into a Medicaid server that went online without proper configurations, the State of Utah had to endure numerous audits conducted by various regulatory entities. The State of Utah DTS lacked the visibility needed to gather accurate, real-time information

Security Solution

- Forescout platform
- Enterprise Manager
- Forescout eyeExtend for Tenable® Vulnerabilty Manager
- Forescout eyeExtend for ServiceNow
- Open Integration Module

Use Cases

- Device visibility
- Asset management
- Device/regulatory compliance
- Network access control
- Incident response

Results

- Non-intrusive, agentless visibility across all devices on the extended enterprise network
- Endpoint compliance thanks to availability of detailed configuration and other device information
- Projected savings of millions of dollars resulting from faster audits
- Complete and accurate asset inventory to support accurate chargeback to state agencies
- Operational improvements within compliance, security, networking, asset management and help desk
- Faster incident response—detection in seconds instead of hours
- Audit efficiencies thanks to single dashboard for management and reporting (for HIPAA, IRS, CJIS, PCI) and integration with ServiceNow CMDB

regarding which devices were on its network, not to mention pertinent compliance details—such as configurations and software versions for each device. Consequently, the audits were extremely time-consuming and costly. In addition, the audit findings continued to highlight shortcomings in security.

The State of Utah DTS knew it needed to improve asset management. Lack of clarity as to what was on the network meant that the organization's ServiceNow® configuration management database (CMDB) could not count on having complete or accurate information. Unknown asset count also made it difficult to justify chargeback amounts on its invoices to state agencies since billing is based on number of devices.

Why Forescout?

POC Converts the Most Adamant Opposition

After learning about the Forescout platform, the State of Utah DTS conducted a 60-day proof of concept (POC) of the solution. Within the first week, without having to install any software agents, the solution had discovered every asset on the network—PCs, laptops, smartphones, routers, switches, printers, and so on. Almost immediately, it also identified critical security gaps or vulnerabilities. For instance, it found 48 percent of devices on the network were vulnerable to WannaCry or WannaCrypt ransomware, 30 devices had peer-to-peer (P2P) applications installed that provide file-transfer capabilities, 92 unclassified or rogue devices existed on the network, and several devices were not running antivirus software.

The rapid deployment, instant and detailed enterprise visibility, and continuous asset situational awareness provided by the Forescout platform impressed even those aligned with Cisco, who ultimately became technical champions for Forescout. The State of Utah DTS team also valued how the solution could work in its heterogeneous environment, including alongside Cisco ISE.

"We wanted something that would 'play nice'," explains Phil Bates, Chief Information Security Officer for the State of Utah. "In addition to being vendor-agnostic, the Forescout solution is quick and easy to implement and provides outstanding visibility, compliance and classification capabilities in real time. Plus it integrates easily with other systems in our organization making them more effective and efficient."

CIO Impressed with Breadth of Potential Applications

In the course of the Forescout POC, the State of Utah DTS team realized it could greatly expand on its initial three use cases (rogue device detection, 802.1X check, and automated remediation). Subsequently, seven additional use cases were added to the POC, including: classification and categorization of devices, automated controls, automated notifications, port and protocol checks, and asset discovery for asset management.

"I could see clearly that every one of my direct reports would have an application for the Forescout solution," said CIO Michael Hussey. "There's no question it would help dramatically in security, compliance and desktop support."

"I could see clearly that every one of my direct reports would have an application for the Forescout platform. There's no question it would help dramatically in security, compliance and desktop support."

— Michael Hussey, Chief Information Officer, State of Utah

Business Impact

Improved NAC, Rogue Device Detection and Faster Incident Response

During the POC, the State of Utah DTS could instantly see devices that shouldn't be on its network, such as an employee's Xbox system. Now such unauthorized devices are automatically removed and not allowed to access the network. The Forescout platform inspects any device that attempts to connect to the network and only allows access if it has been authorized by the State of Utah DTS. Access policies can vary by department, network segment or by device classification per user. For instance, some network segments, such as those used by critical state agencies only allow state-owned devices to gain access.

The DTS is also experiencing faster incident response now. "In the past it took two to three hours to find an infected machine and remediate it," says CISO Bates. "With the Forescout solution, we can find the right machine and shut it down within seconds."

Dramatic Time and Cost Savings with Respect to Audits and Compliance

Perhaps the most measurable benefit of implementing the Forescout solution is the reduction in time and money spent on audits and compliance. With 20 to 30 people involved, the cost in man-hours to create audit reports manually with spreadsheets was well over $1 million every three years. "With the Forescout solution, we expect to save millions from exponentially faster audits that produce fewer findings and require less remediation effort," notes Bates. "And that savings doesn't take into account savings from avoiding a breach, thanks to improved ability to keep endpoints compliant and unauthorized devices off the network."

The state also reaps time savings from consolidating compliance data into one system. Audit data that was present in multiple disparate systems—one for HIPAA, another for the IRS, and so on—is now managed from Forescout's dashboard which provides single-pane-ofglass visibility across the extended enterprise.

Integration with Other Systems Saving Time, Improving Accuracy and Reporting

For the State of Utah, another huge benefit of implementing the Forescout platform is its ability to integrate it with existing security and infrastructure solutions—to enhance their value by exchanging accurate, real-time, contextual information with them about everything on the network, and by increasing operational efficiencies through automation. Consequently, the state is in the process of integrating the Forescout solution with its ServiceNow CMDB using the Forescout eyeExtend for ServiceNow.

In the future, the State of Utah DTS plans to use additional eyeExtend Modules to integrate the Forescout platform with a number of its security and other software tools in its environment. To integrate with legacy or homegrown systems, the state purchased the Forescout Open Integration Module (OIM).

> "With the Forescout platform, we expect to save millions from exponentially faster audits that produce fewer findings and require less remediation effort."
>
> — Phil Bates, Chief Information Security Officer, State of Utah

Extending NAC Policies to Mobile Devices

The State of Utah DTS wanted to extend the visibility that the Forescout solution provides to state agencies' mobile devices—smartphones as well as tablets and laptops in Utah Highway Patrol cars, for instance—which connect directly to a Verizon private network. They decided to see if the Forescout solution would work for this adjunct network as well. It did. As a result, the state's mobile devices can now be protected by the same NAC rules as their equivalent on-premises devices.

Proof to Justify Billing for Technology Services to State Agencies

The availability of accurate, up-to-date information on devices across the network also benefits the State of Utah in yet another way completely unrelated to security, compliance or asset management: billing. To receive payment for the various IT services it provides, the State of Utah DTS bills state agencies based on their number of active devices using the services. In the past, the DTS had no accurate way to prove to an agency the number of devices that were receiving its services. Agencies would dispute their invoices, claiming that they had fewer devices using DTS services than stated, and physically counting devices to justify invoices proved a nightmare.

Today, however, the DTS can substantiate its invoices thanks to its Forescout implementation. "The Forescout solution gives us the ability to point to each agency's exact number of PCs, printers and other devices, and say, yes, we can prove it," says Bates. "We can also provide accurate cost projections and quotes so state agencies can account for IT expense in their budgets and plan accordingly."

Future Uses and Benefits Are in the Works

"The benefits of so quickly and easily being able to see exactly what is on our network at all times, with such granular detail, extend far beyond what we initially thought," concludes Bates. "We are looking forward to seeing how many more ways we can leverage the Forescout solution to make processes more secure and efficient."

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