Case Study

FORESCOUT

OSHPD

California Agency Improves Security Posture Using the Forescout Platform

INDUSTRY

Government

ENVIRONMENT

2,300 wired and wireless endpoints statewide, including IoT devices; two campuses, data center and cloud environments.

CHALLENGE

- Manage security effectively with a small information technology team
- Mitigate risk of data breach
- Shrink gap from incident to response
- Protection against rogue devices and unauthorized access
- Bring endpoints into compliance and keep them compliant

SECURITY SOLUTION

- Forescout platform
- Forescout eyeExtend for ServiceNow

> **The ease of endpoint compliance contributed significantly to preventing intrusion during this exercise. We did extremely well on this aspect of the assessment. Forescout just saw it all."**
>
> **— Ryan Morris, Chief Technology Officer, California Office of Statewide Health Planning and Development**

Overview

To fulfill its mission of improving access to quality healthcare for Californians, the Office of Statewide Health Planning and Development (OSHPD) certifies the safety of hospital and skilled nursing facilities, offers financial assistance to individuals and healthcare institutions and collects and publishes healthcare data. To reduce the risk of a data breach, ransomware attack, or other malicious cyberattacks, the California state agency needed a better way for its small IT staff to more effectively manage endpoint hygiene and block unauthorized access to its network. The Forescout platform provided the continuous device visibility and control needed to bring endpoint compliance up to date and keep it current, safely onboard guests, detect and isolate rogue devices and more. It also improved the accuracy of the organization's asset management database and helped accelerate incident response.

Business Challenge

"We need to know exactly what's on our network at all times, but we simply had no way of doing so."

— Ryan Morris, Chief Technology Officer, California Office of Statewide Health Planning and Development

For its size and network complexity, OSHPD has a small infrastructure team of seven people. "We are always looking for tools that are easy for us to manage and don't require dedicating a full-time person or writing lots of scripts," says Ryan Morris, the chief technology officer at OSHPD.

OSHPD had implemented a major networking vendor's product across its enterprise to create and enforce security policies across endpoint devices. The solution, however, was too complicated for the team to manage effectively. "We really struggled with managing the tool and extracting the type of visibility information we needed from it," explains Morris. "We need to know exactly what's on our network at all times, but we simply had no way of doing so."

Why Forescout?

Impressed by Comprehensive Visibility and Rapid Time to Value

After evaluating potential options for expanding device visibility, OSHPD decided to conduct a proof of concept (PoC) of the Forescout platform. The PoC, which took only a few days, convinced OSHPD to deploy it as soon as possible.

"In less than five days, we were able to see everything on our network—including things we didn't know about—and in greater detail than we ever had before," recalls Morris. "It just blew our team away. The ability to so easily and quickly VLAN a machine and disable USB ports was just the tip of the iceberg."

USE CASES

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

RESULTS

- Rapid time to value—full visibility in five days
- Discovered 28% more devices than expected in asset inventory
- Transformation of endpoint compliance, bringing devices up to date and keeping them current
- High score from California Military Department security assessment
- Accurate, real-time asset inventory through ServiceNow integration
- Several days each month saved in security administration thanks to automation and remote remediation
- Safe onboarding of consultants and BYOD devices
- Faster response to incidents, from one or two days to seconds

> **In less than five days, we were able to see everything on our network—including things we didn't know about—and in greater detail than we ever had before. It just blew our team away. The ability to so easily and quickly VLAN a machine and disable USB ports was just the tip of the iceberg."**
>
> **— Ryan Morris, Chief Technology Officer, California Office of Statewide Health Planning and Development**

Business Impact

Accurate Visibility Detects 28% Additional Devices

"We thought we had around 1,800 devices and the Forescout platform discovered 2,300," notes Matthew Morgan, IT manager of OSHPD. "It found USB thumb drives, external hard drives, lots of smartphones and all our IoT devices, such as security cameras and conference room equipment. The ability to see them all in real time, in one place, and with such granular detail is extremely valuable. We now have so much information at our fingertips about every device—and all without having to deploy agents or write scripts."

Real-Time Posture Assessment Reduces Risk

Continuous monitoring and assessment of endpoints has completely transformed device compliance at OSHPD, dramatically bolstering the agency's overall security posture and reducing risk. "Before implementing the Forescout platform, our antivirus coverage was all over the map; we had multiple versions of the software and some devices were two to three versions behind," remembers Morris. "With the Forescout platform, we rapidly determined exactly which systems needed updating and brought them all into compliance. Now we can easily check endpoint hygiene at any time to keep software versions, Windows updates and patches current across devices."

Easier Compliance Receives High Marks from Red Team and Saves Time

All California state agencies receive periodic independent security assessments. "During OSHPD's assessment, the IT team was able to leverage the Forescout platform to verify that our endpoints were running the latest patches, most recent versions of antivirus software, and so on," explains Morris. "The ease of endpoint compliance contributed significantly to preventing intrusion during this exercise. We did extremely well on this aspect of the assessment. Forescout just saw it all."

The Forescout platform also helps OSHPD detect anomalies and vulnerabilities on endpoints sooner for faster remediation and reduced operational overhead. For example, some group security policies purposefully disabled a couple registry keys. "We assumed that these keys had been disabled on all servers but a compliance check using the Forescout platform showed that a dozen servers lacked the group policy," recalls Morgan.

"We then used the Forescout solution to disable the registry keys and had our service desk fix the problem," continues Morgan. "Before implementing the Forescout platform, we would not have known about this server communication issue, and, had we known, I would have had to manually go and touch every one of those servers. Forescout saved me a day or two of work just on that instance."

Network Access Control Ramps Up Defenses, Safely Onboards Guests

OSHPD doesn't just use the Forescout platform to see; the agency also uses it to control access to its network. If the Forescout platform detects an unknown device attempting to access the network, the device is automatically routed to a guest virtual local area network (VLAN). If malware is suspected, then the device is routed to an isolated VLAN for quarantine and further analysis.

OSHPD also uses the Forescout platform to onboard consultants by routing them to the guest VLAN where they can access the tools they need without being able to access confidential files and systems.

> **Before implementing Forescout, we would not have known about this server communication issue, and, if we had, I would have had to manually go and touch every one of those servers. Forescout saved me a day or two of work just on that instance."**
>
> **— Matthew Morgan, IT Manager, California Office of Statewide Health Planning and Development**

> **Our engineers have been very pleased with the Forescout platform. It's been very easy for them to use and adopt, and they enjoy working with it. It's a great product, and we have only scratched the surface of what it can do."**
>
> **— Ryan Morris, Chief Technology Officer, California Office of Statewide Health Planning and Development**

Trustworthy Asset Inventory and Automated Ticketing

In the past, OSHPD tried to use SCCM for asset management but found it difficult to determine software versions and produce meaningful reports. The agency implemented Forescout eyeExtend for ServiceNow to integrate the contextual data procured by the Forescout platform with the company's ServiceNow configuration management database (CMDB) and help desk system.

"With the Forescout-ServiceNow integration, we can be sure that the data fed into the CMDB from various sources is accurate and current," says Morris. "And asset reports are way more useful than before." In addition, the integration allowed OSHPD to automate help desk ticketing. When the Forescout platform detects a rogue device, for instance, an incident ticket is automatically opened.

Faster Incident Response

"When our endpoint protection software notifies us that an endpoint is infected, I simply right-click on the device within the Forescout dashboard to assign the device to a VLAN and isolate it," explains Morgan. "Within just a minute or two, I've stopped the malware in its tracks."

In the future, OSHPD is considering implementing additional eyeExtend products to integrate the device visibility and control capabilities of the Forescout platform with other systems in the agency to more easily automate policy-based actions and further accelerate incident response. The agency is currently evaluating Forescout eyeExtend for Splunk to enable its SIEM to automatically initiate mitigation actions, such as alerting users, initiating scans by another security tool and sharing real-time contextual information with other systems to accelerate quarantining or other remediation.

Infrastructure Team and IS Administrators Delighted with Platform

OSHPD's infrastructure team and IS administrators rely on the Forescout platform daily. "Our engineers have been very pleased with the Forescout platform," notes Morris. "It's been very easy for them to use and adopt, and they enjoy working with it. It's a great product, and we have only scratched the surface of what it can do."

Learn more at
www.Forescout.com

FORESCOUT

Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591