

## Incident Response &amp; Zero Trust Segmentation



## U.S. State Government Agency

“Within hours of installing eyeSegment, using its traffic visualization capabilities, we were able to pinpoint the attack point of entry and begin to remediate.”

– Chief Technology Officer,  
U.S. State Government Agency

## Environment

10,000 wired and wireless devices across multiple divisions and 220 sites; 4,200 employees

## Industry

Government

## Why They Chose Forescout

- Rapid time to value and proven ROI
- No need for infrastructure upgrades
- Continuous situational awareness
- Rapid incident identification and remediation
- Proven ability to scale and support distributed sites
- Knowledgeable and responsive systems engineers



## HOURS

to determine cause of attack  
and remediate



## WEEKS

saved identifying and  
remediating vulnerabilities



## 13 HOURS

saved weekly on device  
compliance

## Business Challenge

This U.S. state agency was already a happy customer, using the Forescout platform to identify and enforce compliance for 10,000 connected devices across its distributed enterprise. Suddenly, however, they noticed an abnormal increase in authorized users being locked out when they tried to log on. The team suspected malicious activity but couldn't determine the cause. They contacted their trusted Forescout systems engineer, who suggested trying Forescout eyeSegment. Within hours, eyeSegment helped the team identify a compromised laptop belonging to an executive assistant working from home during COVID-19. When logged into the network for legitimate business, the exploited device was being used to perform credential-stuffing attacks.

“Forescout and eyeSegment are at the forefront of our journey to Zero Trust, helping us ensure that only the right people have access to right resources under the right conditions.”

– Chief Technology Officer, U.S. State Government Agency

## Positive Business Outcomes With Forescout

The benefits of complete visibility of devices and traffic at this state government agency are:

- Blocking of rogue and noncompliant devices from accessing the network
- Streamlined compliance with state and federal regulations while reducing time for reporting and operational audits – a task that previously took a minimum of several hours now takes minutes
- Accurate, real-time asset inventory alleviates the need for a \$42,000 asset management tool
- Accelerating the transition to Zero Trust

Download full case  
study to learn more

DOWNLOAD

Contact Forescout today  
to help your organization  
achieve amazing results.  
[references@forescout.com](mailto:references@forescout.com)

Learn more at [Forescout.com](https://forescout.com)

© 2021 ForeScout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents is available at [www.forescout.com/company/legal/intellectual-property-patents-trademarks](https://www.forescout.com/company/legal/intellectual-property-patents-trademarks). Other brands, products, or service names may be trademarks or service marks of their respective owners. Version 01\_21