Case Study

FORESCOUT
Active Defense for the Enterprise of Things™

South Central Power Company

Electric Utility Gains Visibility, Compliance and Zero Trust Network Segmentation with Forescout

$600,000+
saved in three-year ROI benefits

1 WEEK
to discover all devices

5+ MONTHS
saved on asset inventory

South Central Power Co.
A Touchstone Energy® Cooperative

Industry
Utilities/Energy

Environment
1,400 wired and wireless devices across five locations; 250 employees

Challenge

- Lack of visibility into all devices on the network
- Physical segmentation of network causing visibility blind spots
- Compliance with PCI and critical infrastructure regulations
- Confidence that security tools in layered, multivendor defense are doing their job
- Enforce policies without disrupting operations

Overview

South Central Power Company (SCP) is a member-owned electric utility serving more than 120,000 residential, commercial and industrial customers across 24 counties in the U.S. state of Ohio. To provide continuous device visibility, network access control (NAC) and network segmentation, rather than turn to multiple vendors, the company implemented the Forescout platform. With the Forescout solution, the company achieved 100% device visibility and control while simplifying and accelerating the design and deployment of Zero Trust network segmentation and reaping additional efficiencies estimated to save more than $600,000 in three years.

Business Challenge

"Besides helping us to see more clearly, we wanted a 'Big Brother' to double-check our other security tools. We also knew we needed help with segmentation."
— Jeff Haidet, Director of Application Development and Architecture, South Central Power Co.

Despite its multilayered defense and multivendor security stack with best-of-breed security tools, South Central Power Company still had no idea how many devices were on its network. To protect personally identifiable information (PII) and business operations and comply with PCI regulations, the SCP security team knew they needed a way to continuously identify, segment and enforce compliance of every connected thing on its heterogeneous network. They also desired a way to validate that other security tools in the environment provided accurate information and performed as intended. In addition, SCP staff suspected that the corporate network's physical design hindered security but did not know how to confirm the problem or implement more logical segmentation.

Security Solution

- Forescout eyeSight
- Forescout eyeControl
- Forescout eyeSegment
- Forescout eyeExtend for Carbon Black

Use Cases

- Network access control
- IoT security
- Network segmentation
- Asset inventory
- Device compliance
- Security orchestration

Results

- Rapid time to value – full visibility and 100% device classification in weeks
- Continuous, comprehensive visibility across all network-connected things
- Accurate, real-time asset inventory system replaced cumbersome manual method
- Simplified, accelerated Zero Trust network segmentation, thanks to a clear understanding of traffic flows and ability to simulate policy changes
- Ability to switch network hardware without penalty due to vendor-agnostic visibility
- Oversight to validate other security tools in the environment
- Zero Trust NAC to block rogue and noncompliant devices
- Visibility and control that aids both security operations and networking teams daily
- Significant ROI – $612,500 three-year savings projected

Why Forescout?

During an independent penetration test that reconfirmed the need for better visibility and NAC, the pen tester highly recommended Forescout. They implied that if the Forescout platform is on site when they arrive, it has already done their job. This glowing recommendation led the company to learn more about the solution, which led to a deep-dive proof of concept. "As soon as we saw and understood the power of the Forescout platform to bridge visibility and control security gaps – and of eyeSegment to noninvasively rectify segmentation shortfalls – we knew that it was what we were looking for," claims SCP Manager of Applications and Security Jeff Haidet. "Vendor independence was also a huge selling point because we are constantly upgrading or replacing networking hardware."

Business Impact

Comprehensive Visibility Opens Eyes and Overhauls Asset Inventory

The Forescout platform was up and running and providing granular visibility in hours. The SCP security team then let it run for a week. It discovered a total of 1,400 endpoints – an average of seven to eight endpoints per employee, which made a significant impression on senior management. The system auto-classified 85% of the devices, with the remaining devices classified shortly after that. Without the Forescout platform, locating and classifying all devices in the company's five locations would have easily taken six months, if it happened at all. Such comprehensive, real-time visibility allowed SCP to scrap its inaccurate, paper-based asset inventory process. Processes for onboarding and offboarding equipment also improved dramatically.

Non-Disruptive Approach to Zero Trust Segmentation

To improve segmentation, Haidet and his team turned to Forescout eyeSegment. "We used eyeSegment to map traffic flows and determine which devices, users and services on the network need to talk to each other," explains Haidet. "The ability to logically define segments, as opposed to physically defining them, accelerates visibility into behavior. For example, eyeSegment showed us how two different groups of devices were passing information back and forth from one switch port to another undetected because their communication never hit a gateway. So, we moved gateways to gain the visibility we need. It is also helping us redesign our physical segmentation and do so noninvasively. We can simulate policies to see if anything breaks, and fine-tune and re-simulate as needed before we actually implement."

Oversight for Device Compliance and Security Tool Validation

SCP security uses the Forescout platform to continuously monitor endpoints for the presence of appropriate antimalware agents and patching, as well as for critical vulnerabilities or unauthorized apps like Dropbox. If a device does not comply with corporate policy, the Forescout platform blocks it from accessing the corporate network or pushes it to the guest network. "When the Covid-19 pandemic caused most of our employees to work from home via VPN, the ability to continue monitoring their device's compliance became even more important," notes Haidet. "In addition, Forescout lets us double-check that the pieces of our layered security stack – from firewall to switch to antivirus – are doing what they need to be doing."

> "To gain the functionality that Forescout provides—from seeing and managing assets to triggering control actions and accelerating Zero Trust segmentation—we would have needed multiple tools. Going with Forescout was far more cost-effective."
>
> — Jeff Haidet, Director of Application Development and Architecture, South Central Power Co.

A Truly Collaborative Partnership and Undeniable Business Value

At South Central Power Company, both security operations and networking teams rely on the Forescout platform daily. "The Forescout team is also an extension of what we do," notes Haidet. "We have a truly collaborative relationship – which is very difficult to achieve with vendors when you acquire new tools. I think we've hit a homerun here. With just 250 employees, we're small potatoes for Forescout. However, the level of support and commitment Forescout has given us makes us feel like a Fortune 100 company."

To quantify the economic benefit of turning to Forescout, Haidet used a customer-based ROI tool developed by IDC. The ROI analysis showed $612,500 savings over three years from IT staff efficiencies, risk mitigation and business productivity benefits and IT infrastructure cost reductions. When talking with peers, Haidet tells them: "Forescout is your vendor-agnostic, 'one-stop oversight shop.' The bigger your network gets, the bigger the cost savings and stronger your case for it becomes."

FORESCOUT
Active Defense for the Enterprise of Things™

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