Case Study

Financial Services Firm Counts on ForeScout for Device Visibility, Policy-Based Segmentation, Threat Response and Compliance Enforcement

INDUSTRY

Financial Services

ENVIRONMENT

Headquarters plus 100 branches with 12,000 connected devices comprising Windows PCs and virtual machines, ATMs, cash-management devices, teller machines, cameras, stock tickers and more.

TECHNICAL CHALLENGES

- Identify, classify and manage connected devices on the network
- Ensure device hygiene without impeding services or transactions
- Comply with FDIC, GLBA, PCI and other regulations
- Protect confidential customer information
- Securely accommodate BYOD and guest endpoints
- Maximize value of existing network and security tools
- Improve security posture while reducing total cost of ownership

Overview

A growing financial services firm with approximately 100 branch offices in the southeastern United States requires a heterogeneous network that is both flexible and tightly secured. As you'd expect, the firm's 2,600 employees use all kinds of network-connected devices, including corporate-owned PCs as well as personally owned (BYOD) smartphones and tablets. IoT devices such as ATM machines and security cameras are also part of the mix, which comprises around 12,000 connected endpoints on any given business day.

Prior to 2016, the firm had been depending on a network access control (NAC) solution that was by all accounts primitive. Anyone logging on would be directed to a guest registration page and either granted access to an Internet-only guest network or to the internal network. But that was about all it could do. For a whole host of reasons, the company's SecOps team wanted much more.

Business Challenge

There's no way around it: financial institutions will always be prime targets for cybercriminals. And that makes their security requirements extremely complex. Confidential customer data must be protected at all costs. Compliance with multiple regulations has to be a given. And, literally, the company has to be open for business: the network must be secure yet readily available to employees, customers and contractors. Specifically for financial institutions, the challenges include:

- Preserving customer trust by protecting data privacy
- Maintaining a strong security posture without impeding business operations
- Staying in compliance with FDIC, GLBA, PCI DSS and other regulations
- Adding new types of devices and services to networks without adding vulnerabilities
- Ensuring that connecting and already connected devices meet baseline compliance requirements
- Accommodating BYOD and guest endpoints without compromising security
- Orchestrating existing security tools into a unified solution that accelerates incident response and reduces vulnerabilities

Why ForeScout?

The company's previous technology left a lot to be desired. An older-model Bradford Networks product, it was a basic tool that wasn't suited to a banking environment that required an intelligent, feature-rich cybersecurity solution. The firm's Deputy CISO and his SecOps team knew better solutions were out there. Cisco ISE was briefly under consideration, but it wasn't seen as a solution they could deploy quickly. Besides, the word on the street was that the Cisco product was difficult to use. In contrast, the Deputy CISO had nothing but good experiences with the ForeScout platform while working for one of the U.S.'s biggest

SOLUTION

- 6 ForeScout CounterACT® appliances deployed in clusters in the company's primary data center and failover data center
- ForeScout Enterprise Manager
- ActiveCare™ Advanced Support
- ForeScout Extended Module for Palo Alto Networks WildFire™
- ForeScout Extended Module for IBM® QRadar®
- ForeScout Extended Module for Rapid7® Nexpose
- ForeScout Extended Module for ServiceNow®
- ForeScout Extended Module for VMware® AirWatch®
- ForeScout Open Integration Module (OIM)

RESULTS

- Fully operational in less than two weeks
- Real-time visibility and policy-based control of networked devices
- Automated security and compliance controls, reducing manual tasks
- Orchestration between CounterACT and existing security tools
- Optimized network segmentation planning and implementation
- Streamlined asset inventory and reporting
- Improved device management and regulatory compliance
- Gained $415,737 in average annual benefits*
- Realized $215,458 in IT staff efficiencies*

*Calculated by ForeScout Business Value ROI Tool using IDC methodology

healthcare service providers prior to joining the financial services firm, and he's still very positive.

"Not only can ForeScout isolate devices and do network segmentation, it can also discover networks that haven't been seen previously," he said. Then he rattled off other reasons:

"It can push scripts. It can discover detailed information. It builds inventory over time of what you're seeing. You can switch VLANs on the fly. I mean, it's a powerful tool. It does what you tell it to do."

And perhaps most important, there's visibility—agentless visibility. When the SecOps team decided to bring in ForeScout for a proof-of-value assessment and got their first look, they were amazed at what the platform revealed about endpoints on the network.

"We were seeing devices we didn't know we had," said the SOC Manager. "There were old legacy networks that people thought were decommissioned that still had some log devices on them. We were getting to see all the different devices at the branch-office level—all kinds of things that weren't previously documented."

Once the team decided to move forward with ForeScout, deployment went smoothly. With the ForeScout platform in place, it was just a matter of getting the appliances connected to the core, standing up the network segments and configuring policy. The company chose a centralized deployment model that runs ForeScout appliances at the corporate data center's core switch and replicates a failover cluster at its backup data center. The ForeScout platform has full access to the company's entire switching infrastructure as well as all virtual devices. "We had it fully operational in about two weeks—at least for the initial requirement of segmenting devices off the network that weren't supposed to be there," commented the company's SOC Analyst.

With 2,600 employees at 100 locations all using multiple devices running a slew of applications—not to mention thousands of customers, contractors, analysts, regulators and media representatives plugging into the network every day—it's no wonder the SecOps team appreciated the agentless visibility they gained with ForeScout.

Business Impact

For this financial services firm, the ForeScout platform provides intelligent functionality that fits the bill on multiple levels.

Device Identification, Inspection and Isolation – The Deputy CISO and his team appreciate the ability to see the device and classify its type, understand how long it has been on the network, identify open ports and more. He noted that his team recently used the ForeScout platform to isolate a device on the network to stop it from beaconing out to a command-and-control server and pulling in more malware.

Advanced Threat Detection and Containment – The company's threat detection and response solution is built upon a combination of the ForeScout platform and a ForeScout Extended Module that provides orchestration between Palo Alto Networks' WildFire™. "When WildFire detects a malicious file or executable attachment, it sends the indicator of compromise to the ForeScout platform, which can check other devices or inspect network traffic for similar IOCs. If anything is found, ForeScout quickly places the device in an Internet-only VLAN

> **Before we were primarily focused on detecting rogue devices, isolating them off the network and sending us an alert. The addition of ForeScout visibility and scripting has been awesome. It's a huge tool in our arsenal that we didn't have previously."**
>
> — SOC Analyst

where it can't cause harm to other corporate systems or access our resources," explained the SOC analyst. This dynamic segmentation is made possible through deep integration with more than 20 wired and wireless switch vendors, and is just one of the policy-based control actions possible on the ForeSout platform.

Event Correlation, Analysis and Response – The SOC team also combines the intelligence of the ForeScout platform with its QRadar® security information and event management tool via the ForeScout Extended Module for QRadar. According to the SOC Manager, the team feeds all ForeScout logs into the QRadar instance where devices get isolated. Then they do correlations on all the data. If the combined solution detects something, it generates alerts to let them know.

Scripting and Auditing – The SecOps team uses the ForeScout platform to verify that managed devices are running Trend Micro full-disk encryption as well as Carbon Black antivirus and other security applications. In addition, the SecOps team uses the ForeScout platform to deploy these security tools to new systems or ones that require remediation. "We just write a script saying "Install this software," said the SOC Manager. "We push it out and then we use ForeScout to audit to make sure our security tools are installed. The ability to automatically run scripts based off certain policies is huge…The addition of the visibility and the scripting has been awesome."

Auditing and compliance – The ForeScout platform can run reports about assets on the network and determine whether they are up to corporate and regulatory bodies' standards. It can quantify how many endpoints of a certain type are connected—how many Windows 7 or Server 2003 devices are still on the network, for example. The SecOps team generates reports for their own purposes as well as for FDIC auditors and others. To aid further in regulatory compliance, ForeScout's custom policy engine can identify thousands of IoT devices—providing accurate, real-time inventories of the full range of network-connected devices to demonstrate compliance with SOX, PCI DSS and other regulations.

Managing disparate technologies resulting from acquisitions – The firm is growing rapidly, partly due to acquisitions. Its standard practice is to isolate network infrastructure that results from acquisition and "forklift" it to a completely new network. During the transition period, it's not uncommon for employees to try to connect their old devices. The ForeScout platform automatically isolates these endpoints and notifies users that there's an issue: namely, that their equipment is unauthorized, unsanitized and unfit for the network until appropriate hygiene measures are taken. It's one more way the ForeScout platform helps to ensure device compliance.

Inventorying assets – The company's IT department is in the process of standing up a ServiceNow® configuration management database (CMDB) and using the ForeScout Extended Module for ServiceNow to integrate the CMDB with the ForeScout platform. When the process is complete, the ServiceNow CMDB will be able to leverage ForeScout's real-time visibility and up-to-date intelligence when it comes to device properties, classification, configuration and compliance status. This will enable the SecOps team to get a current view of networked assets, track their movement and remediate or retire those assets as required. In this way, the firm can gain a trusted data set, improve asset compliance and provide the basis for informed business decisions.

> **The ForeScout platform discovers devices and captures detailed information. It builds inventory over time of what you're seeing. You can switch VLANs on the fly. I mean, it's a powerful tool. It does what you tell it to do."**
>
> — Deputy CISO

Orchestrating security by sharing intelligence – Over the years, the company has made significant investments in SIEM, VA, ATD, AV and other key security tools. Through integrations made possible by ForeScout Extended Modules, the network environment is now able to share contextual device data between the ForeScout platform and these security products—automating policy enforcement across disparate solutions, bridging previously siloed IT processes and accelerating system-wide incident response.

Business Value

The return on investment of a technology that has been recently deployed is difficult to measure no matter what solution is being analyzed. However, in an effort to quantify the economic value of using the ForeScout platform to gain device visibility, automate threat mitigation and policy compliance, improve overall IT efficiency, and reduce risk, IDC recently interviewed ForeScout customers and completed an extensive business value analysis. ForeScout then used IDC's methodology to develop an ROI tool which this financial services firm's SecOps team used to calculate monetary benefits. Figure 1 below summarizes those benefits.

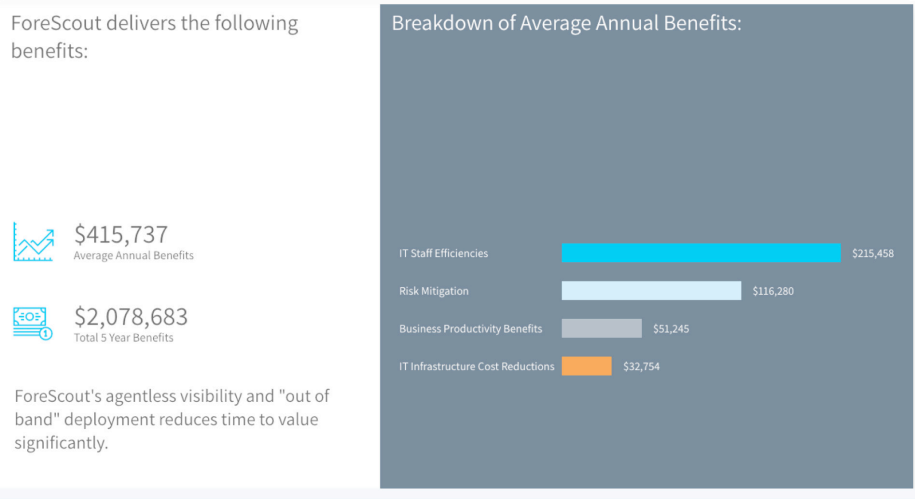

Figure 1. A summary of return on investment using the ForeScout ROI tool (based on IDC methodology), as determined by the firm's SecOps team.

Learn more at
www.ForeScout.com

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