ForeScout®

Solution Brief

Financial

Boost security, privacy and compliance while maintaining availability of financial services networks

The security requirements of networks in financial institutions are extremely complex. Confidential customer data must be protected at all costs. Compliance with regulations must be demonstrable. And, like any business, the network must be secure and available to employees, customers and contractors. ForeScout achieves this by providing secure access to PCs and laptops, mobile devices and other endpoints while giving IT personnel the tools to see, control and orchestrate network security.

Business Challenges

- Preserve customer trust by protecting data privacy
- Demonstrate regulatory and security policy compliance
- Improve security posture while reducing total cost of ownership

Technical Challenges

- Control access to confidential data
- Measure effectiveness of security controls
- Identify and secure unmanaged and IoT devices
- Guard against targeted malware threats

> “ForeScout provides JPMorgan Chase with enhanced visibility and control across the hundreds of thousands of devices connected to our corporate network.”
>
> **— Rohan Amin, Global CISO, JPMorgan Chase & Co.**

The Challenge

Traditional network security focuses on blocking external attacks with firewalls and intrusion prevention systems. But today, attacks can come from all directions, including internal sources. In fact, misuse and abuse of corporate data resources by employees and contractors are rampant. Traditional methods won’t stop internal zero-day attacks and advanced persistent threats from scanning your network for information.

Similarly, traditional endpoint security systems, such as antivirus, patch management and encryption, provide much-needed endpoint protection but are limited to managed endpoints—ones that contain agents. And, oftentimes, these security systems may not even be fully operational and up-to-date on those endpoints. In many cases, banned endpoints can slip through security, and vulnerable old Windows XP systems can log on undetected as well.

Without a specialized, network-based visibility and control solution, IT managers can be unaware of a significant percentage of network devices, including Internet of Things (IoT) devices such as security cameras, VoIP phones, digital signage, smart printers, facility management devices and more—some of which can be hacked in as little as three minutes.[1] In addition, without proper visibility, failure to identify compromised endpoints is unavoidable, and there is no defense against unseen rogue wireless access points that can extend your network without your knowledge.

Companies in the financial sector must maintain a fine balance between securing customer data and providing customers with 24-hour access to their accounts through multiple channels. Extensive communities of vendors, partners and consultants must be accommodated as well—all with vastly different computing needs and restrictions. And then there are regulatory requirements. In the U.S., under Securities and Exchange Commission rules, firms have to maintain records of employees’ business communications and make sure those records can be readily retrieved and reviewed. Financial institutions that allow employees to

> Interviewed organizations reported identifying 24% more network devices as "known devices" with ForeScout, and being able to take proactive steps to help ensure the compliance of 18% more devices."
>
> — Business Value of ForeScout, IDC – December 2016

use their own devices for work must ensure that the organization can still locate, access and retrieve relevant data when needed. Given these mandates, many institutions block access to BYOD endpoints.

Unfortunately, There's More Than One Way to Rob a Bank

Here are just a few of the most recent pieces of evidence that the keys to minimizing the impact of cyberattacks against financial institutions—or any organizations—are visibility, early detection and rapid incident response.

- Over a weekend in November 2016, money was taken from 20,000 customers' accounts at the UK's Tesco Bank. Upon discovery of the breach, Tesco halted all online payments and confirmed that some accounts "have been subject to online criminal activity, in some cases resulting in money being withdrawn fraudulently." The amount of pounds stolen was not disclosed.[2]
- An attack on the Society for Worldwide Interbank Financial Telecommunication (SWIFT) in May 2016 involved possible computer breaches at as many as 12 banks in New Zealand, the Philippines and Vietnam that are linked to SWIFT's global payments network and that have irregularities similar to those in the February 2016 theft of $81 million from the Bangladesh central bank. The Bangladesh attack, in which the Federal Reserve Bank of New York was tricked by fake SWIFT messages into wiring money it held for the South Asian country to hacker-controlled accounts in the Philippines, is the largest known cyber-heist in history.[3]
- In July and August 2016, 12 million baht (US$350,000) was stolen from ATMs in Thailand in a "jackpotting" spree. The attack was initiated by a team of hackers that breached the state-owned Government Savings Bank's internal network and tricked the software distribution server into delivering malware to ATMs. Then, using modified payment cards, a second team installed malware onto 21 ATMs and made them issue cash in lots of 40,000 bahts ($1,160).[4]
- A Distributed Denial of Service (DDoS) attack in September 2016 on cloud-based Internet performance management company Dyn caused disruption to Twitter, Spotify, Netflix and other online services worldwide. The attack originated from at least one Mirai Internet of Things (IoT) botnet, and Dyn estimated as many as 100,000 endpoints were involved.[5]

These attacks offer proof—if anyone needed it—that cybersecurity threats to financial institutions are real and global. Cybercriminals the world over know how to target financial networks and unsecured endpoints, including IoT devices. All banks and financial services organizations are at risk.

The ForeScout Solution

ForeScout CounterACT® reduces the risk of data breaches and malware attacks. It continuously monitors endpoints on your network, improves the effectiveness of your security policies, and even provides templates to validate compliance with FINRA*, GLBA*, PCI DSS*, SOX* and other regulations. In fact, you can automate endpoint system compliance: CounterACT automatically discovers corporate-owned endpoints that do not have the required antivirus (AV) security software or that have out-of-date security software installed. It provides this intelligence to the centrally managed AV engine and can install or update the AV software on non-compliant hosts in order for them to regain compliance. CounterACT also enables one-click access to reports for auditors.

> “CounterACT delivered value from day one. As soon as it came online we saw our 2,000 endpoints light up on the screen. From there, it only got better as we automated the management of these endpoints and created reports and audit trails generated at the click of a button.”
>
> **— Brian Meyer, Information Security Officer, Meritrust Credit Union**

> “We call CounterACT the ‘Swiss Army knife’ of our information security department, as it facilitates multiple, automated security checks and compliance controls in the most efficient way.”
>
> **— Ali Kutluhan Aktas, Head of Information Security/Risk Management at KKB**

See ForeScout CounterACT delivers real-time visibility of devices on your network. It lets you see devices other solutions can’t (including PCs, smartphones and non-traditional devices) the instant they connect to your network, without requiring software agents or previous knowledge of those devices. It profiles and classifies devices, users, applications and operating systems. What’s more, it identifies, classifies and monitors IoT and other unmanaged devices, ports and connections that reside on financial networks. In fact, since CounterACT’s custom policy engine makes it possible to discover networked devices based on known characteristics, it can automatically identify thousands of IoT devices—saving valuable time by providing IT teams with accurate, real-time inventories of network-connected devices to demonstrate compliance with SOX, PCI DSS and other regulatory agency requirements.

Control CounterACT delivers unparalleled network access control. Unlike systems that flag violations and send alerts to IT and security staff, CounterACT enforces access control policies, endpoint compliance (including public-facing systems such as lobby kiosks and ATMs) and mobile device security. Should a contractor’s laptop be non-compliant with security policies (for example, missing security updates, lacking up-to-date antivirus software or exhibiting anomalous behavior), the device can be isolated to a secure self-remediation portal and not re-admitted to the network until the user has been informed and taken steps to fix the problem.

For corporate-owned devices, CounterACT can automatically perform remediation. It can also enforce guest access agreements and inform staff of equipment-use policies prior to granting access. Customers can be automatically limited to a guest network segment and can readily access financial services without compromising security. Likewise, visitors can be given Internet access through a guest VLAN, and lobby kiosks and other IoT endpoints can be placed on secure segments that cannot touch operational financial systems or confidential customer information.

Orchestrate ForeScout extends CounterACT’s agentless visibility and control capabilities to leading network, security, mobility and IT management products via ForeScout Extended Modules. For example, integration between CounterACT and advanced threat detection solutions can automatically isolate an infected system to a secure VLAN or instantly drop the system’s port, preventing it from spreading malware or communicating with command and control servers to exfiltrate data or propagate malware across the network.

Security information and event management (SIEM) systems can detect suspicious behavior by a device or user and automatically launch policy-based enforcement or remediation actions with CounterACT. That means if a security camera or other IoT device begins navigating the network and attempts to access an accounting system, automated polices can isolate the system and notify security personnel with the identity and exact location of the device.

Here’s how:

1. IoT device connects to the network.

2. CounterACT discovers the device, determines type of device and ownership.

3. If the IoT device is corporate-owned, CounterACT places it in the appropriate VLAN or applies an ACL to limit network access to necessary resources only. If the device is not corporate-owned, it is denied access.

4. CounterACT monitors the IoT segment for anomalous behavior, leveraging a third-party Security Information and Event Management (SIEM) system through a ForeScout Extended Module for SIEM.

5. Based on policy, if one of the third-party systems reports malicious behavior, the IoT device(s) is moved to a restricted VLAN segment for further analysis.

Learn more at
www.ForeScout.com

This ability to orchestrate information sharing and operation among multivendor security tools tears down security silos, allowing you to:

- Share context and control intelligence across systems to enforce unified network security policy
- Automate workflows and processes for quick, coordinated incident responses
- Gain higher return on investment from your existing security tools while saving time through workflow automation

CounterACT is proven in customer networks exceeding one million endpoints. This scalability is especially attractive in banking environments, where distributed branches are the norm, and where mergers and acquisitions are commonplace.

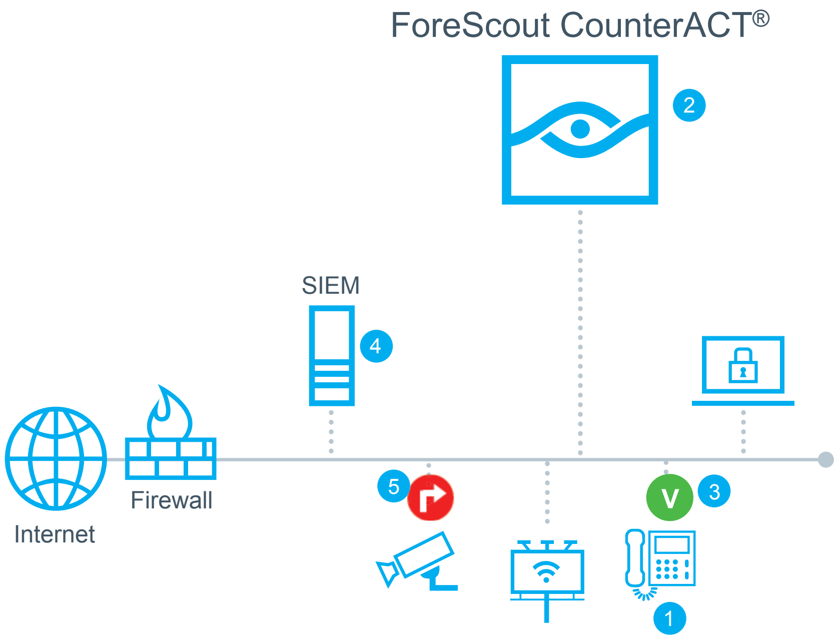

Figure 1: How ForeScout CounterACT applies policy-based security segmentation to IoT devices and quarantines malicious activity.

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
Fax 1-408-371-2284

[1] 2016 ForeScout IoT Enterprise Risk Report, https://www.forescout.com/company/resources/iot-enterprise-risk-report/

[2] November 2016, BBC News, http://www.bbc.com/news/business-37891742

[3] May 2016, Bloomberg Technology, https://www.bloomberg.com/news/articles/2016-05-26/swift-hack-probe-expands-to-up-to-dozen-banks-beyond-bangladesh

[4] August 2016, bankinfosecurity.com, http://www.bankinfosecurity.com/ripper-malware-likely-fueled-thai-atm-attacks-a-9370

[5] October 2016, The Guardian, https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

* FINRA (Financial Industry Regulatory Authority), GLBA (Gramm-Leach-Bliley Act), PCI DSS (Payment Card Industry Data Security Standard), SOX (Sarbanes-Oxley Act)

Version 11_16