FORESCOUT

Financial

Stay secure and compliant while scaling technology and availability needs

Business Challenges

- Serve the business needs securely as technology demands evolve
- Minimize security risk and protect the business reputation
- Demonstrate regulatory and security policy compliance
- Preserve customer trust by protecting data privacy
- Improve security posture while reducing total cost of ownership

Technical Challenges

- Address risks to critical applications and processes across the entire network
- Continuously identify, classify and understand the status of all network-connected devices without disrupting the business
- Ensure dynamic but controlled network access and segmentation without hindering daily activities of employees, customers, partners and guests
- 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 security requirements of networks in financial institutions are extremely complex. Security and availability must match the speed of business. Regulatory compliance must be demonstrable. Business risk must be minimized and confidential customer data must be protected at all costs. And, like any business, the network must be secure and available to employees, customers and contractors without disruption. ForeScout achieves this by providing agentless device visibility, in-depth intelligence, continuous monitoring and automated control that scales across the campus, data center, cloud and mobile workforce.

The Challenge

Financial services firms must innovate to succeed. They face intense pressure to develop cutting-edge services while providing on-demand scalability and ensuring technology availability to a growing number of services and users. The big challenge is how to dynamically extend security and compliance while minimizing technological complexity across evolving business architecture that increasingly seeks elasticity in the cloud. The right solution must safeguard vital business processes, applications, infrastructure and data. Also, it has to minimize disruption and streamline compliance while scaling to meet changing needs and support business agility.

Don't Forfeit the Need for Business Speed to be Secure and Compliant

Without a continuous visibility and control solution, the elastic technology usage of compute, network, storage and mobility assets in financial services introduces security blind spots and non-compliant devices into your environment. Of course, those non-compliant devices are potential entry points for hackers. And as critical applications increasingly interconnect and access each other's information, they add "east-west" traffic that circumvents many security controls, increasing the possibility that malware spreads and threats go unchecked.

To overcome these hurdles, a security solution needs to provide comprehensive visibility across all elastic technology resources using the same people and processes. This visibility must continuously offer insight in device and application security status as well as asset intelligence to eliminate blind spots, build the foundation for proper controls and facilitate asset inventory and tracking. And lastly, the solution should protect without slowing access to critical business services.

FORESCOUT

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."

— IDC Report, *The Business Value of ForeScout,*

Minimize security risk exposure as you embrace operational agility

One of the key priorities of a financial services firm is to protect its assets, data, and applications while establishing the right balance of controls. Understanding your control status while meeting the business demands in an elastic technology environment is significantly harder. Adding devices, servers, virtual machines and access to clouds hinders visibility, fragments control and adds business risk—all of which make it harder to stay in compliance.

Security solutions for financial services need to help consolidate control with a central view of the overall security posture. To effectively manage risk, security professionals need to identify the most critical processes, applications and technologies and match them with prioritized protections. Proper governance requires thoughtful intelligence to carefully build strict controls, including network segmentation to protect the "east-west" traffic and device access controls to restrict the threat access potential.

The ForeScout Solution

ForeScout offers a security solution that provides visibility and posture status into extended network environments, while consolidating control to reduce risk and maintain compliance. As devices connect to the network, data center or cloud, The ForeScout platform gains asset intelligence and verifies their compliance to corporate policies. This intelligence builds the secure foundation for verified asset management and continuous device compliance, as well as scalable, non-disruptive network control and segmentation practices.

In addition, asset intelligence secures the network against targeted breaches that can result in financial losses, stolen data and operational downtime. The ForeScout platform continuously monitors endpoints on your network to refine your security policies to validate compliance with frameworks and regulations such as MiFID II, GDPR, SWIFT CSP, FFIEC, SOX, and NYDFS.*

In fact, the ForeScout platform can automate endpoint system compliance by automatically discovering 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. The platform can even expose potential vulnerabilities in "unpatchable" IoT devices (building automation, security and business machines, etc.), which helps when creating policies for the correct governance actions.

See Understand your security and compliance posture in real time across dynamic physical and virtual infrastructures. In Financial firms, this poses challenges as their networks are dynamic and ever-changing. With ForeScout's active and passive techniques, you gain continuous, in-depth visibility into the connected devices on your wired and wireless networks as well as virtual server instances running in private or public clouds. The ForeScout platform discovers and classifies devices and virtual machines the instant they access your network—without requiring software agents or previous device knowledge. It assesses device hygiene and continuously monitors security and compliance posture. And it quickly evaluates devices and applications, determining the device users, system, configuration, applications and presence of security agents. This saves time by providing accurate, real-time inventories of network-connected devices. It also provides a foundation to easily

FORESCOUT

> **Not only can ForeScout isolate devices and do the network segmentation, it can also discover networks that haven't been seen previously,"**
>
> — Deputy CISO, US National Financial Firm

demonstrate compliance with regulatory agency requirements and drive accurate access control, enforcement and remediation policies.

Control **Consolidate control to protect prioritized assets and minimize security risk.** Once you gain the in-depth visibility into the devices on your network, the ForeScout platform enables a broad range of controls. It lets you automate policy-based access and enforcement—allowing, denying or limiting network access based on device posture and your security policies. It also helps you find and fix endpoint security gaps, alert or quarantine devices based upon anomalous behavior and help maintain and improve compliance with industry regulations. And should you choose to isolate various devices to various network segments or VLANs, the ForeScout platform simplifies this process.

Orchestrate **Share information and automate workflows with third-party solutions.** ForeScout extends our platform's agentless visibility and control capabilities to leading network, security, mobility and IT management products via more than 20 ForeScout Extended Modules.** The ForeScout platform also provides heterogeneous support of wired and wireless switching and routing infrastructure. This ability to orchestrate information sharing and operation among multivendor security tools and network hardware 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

Centralized Management and Control

ForeScout Enterprise Manager provides you with a single pane of glass to centrally manage and control multiple CounterACT appliances in large network environments, all without the need to purchase an additional physical appliance as it's also available for virtual deployment. This gives overall visibility and control of devices and VMs across your campus, data center and clouds—streamlining your operations across your enterprise.

Scale

ForeScout 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.

Here's how:

1. IoT device connects to the network.
2. ForeScout discovers the device, determines type of device and ownership.
3. If the IoT device is corporate-owned, ForeScout 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. ForeScout 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.

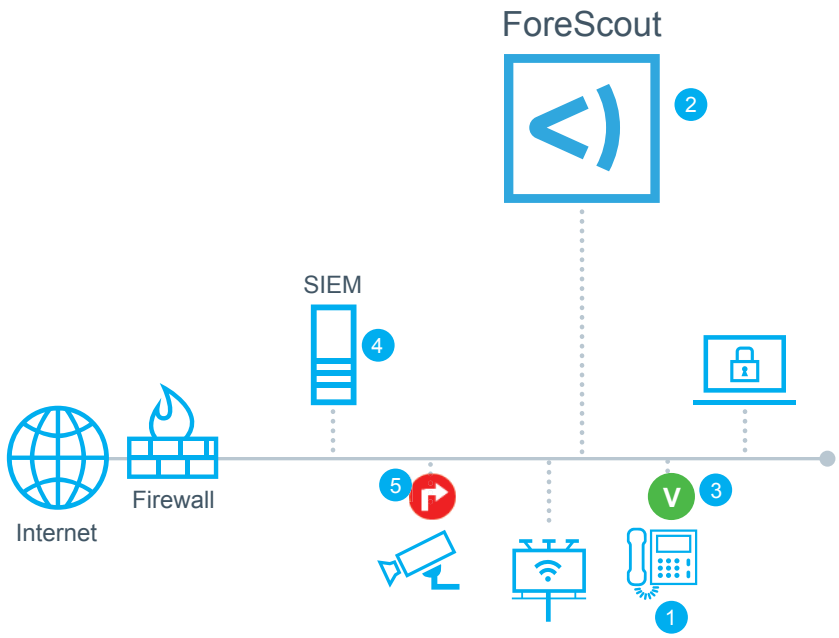

Figure 1: How ForeScout CounterACT applies policy-based security segmentation to IoT devices and quarantines malicious activity.

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

Regulation (GDPR), SWIFT Customer Security Programme (CSP), Federal Financial Institutions Examination Council (FFIEC), New York Department of Financial Services (NYDFS)

** As of March 31, 2018