FORESCOUT

Meeting FFIEC Requirements

Simplify FFIEC compliance and mitigate risk with the ForeScout platform

Business Challenges

- Scale technology to address rapidly changing business needs
- Gain visibility into end-to-end controls across the network to understand risk to critical applications
- Limit attack surface and risk of breach
- Manage change which can be risky and costly
- Balance the need to comply with multiple regulations with rapid deployment of effective technology
- Ensure dynamic network access and segmentation without hindering daily activities of employees, customers, partners and guests

Technical Challenges

- Gain comprehensive visibility into device classification, context and network access
- Mitigate vulnerabilities real time
- Prevent unauthorized applications and devices on the network
- Respond rapidly to breaches to satisfy incident-reporting requirements

A costly breach can break the bank: The average cost of a breach in 2017 was $3.6M.[5]

While pressures intensify to expand technology footprints to support corporate strategies, cyberattacks against financial services institutions continue. Security strategists must also comply with ever-changing regulatory demands while providing visibility into their compliance programs to their boards of directors. ForeScout can help you reduce risk and improve compliance by providing real-time visibility into devices that connect to your financial networks while automating policies to control access to sensitive data and devices.

The Changing Threat and Regulatory Landscape

Responding to regulatory pressures is not new to financial institutions. The Financial Services Sector Coordinating Council (FSSCC) estimates that financial institutions are impacted by up to 24 federal and state regulatory, oversight and examination agencies and self-regulatory organizations with their own independent cyber initiatives.[1]

The changing IT landscape with cloud adoption, IoT and increasing IP-enabled devices brings added challenges to ensure controls are compliant.

Mitigating risk across the expanding attack surface requires a coordination of both cybersecurity and IT management tools. IT audit and security teams are struggling to get a complete view of control gaps and effectiveness.

FFIEC Requirements

The Federal Financial Institutions Examination Council (FFIEC), established on March 10, 1979, is a five-member interagency body that prescribes uniform principles, standards and report forms for the federal examination of financial institutions.[2] The organization publishes a series of handbooks, the most relevant to IT security being the Information Technology Examination Handbook (IT Handbook). This booklet "describes processes and controls that an institution can use to protect information and supporting systems from various threats."[3] Financial institutions are also encouraged to perform a self-assessment with the CyberSecurity Assessment Tool (FFIEC CAT) to help institutions identify their risks and determine their cybersecurity preparedness.[4]

> **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.

Balancing Technology Elasticity with Managing Risk

Banks must compete in a very demanding consumer and commercial space. Technology elasticity satisfies the need for more compute, network, storage and mobile capability. This expansion must occur at the speed of business. Unfortunately, regulations are beginning to catch up with the rapid expansion. Fines are increasing and the need to document and prove effective risk management policies and procedures is critical to complying with these regulations. Scaling effectively while reducing risk requires: 1) comprehensive asset intelligence, 2) automated policy compliance directed at devices as they access the network, and 3) technology tools that can be orchestrated to provide results leading to effective decision-making and rapid incident response.

Asset Intelligence – What You Can't See Can Hurt You

The diversity of devices that connect to your financial networks continues to increase. Along with mobile devices, laptops and servers, non-traditional IoT devices such as VoIP phones and security cameras increase the number of potential threat vectors. Most regulatory bodies, including the FFIEC, require organizations to accurately inventory and classify assets, including hardware, software, information and connections. Relying on inaccurate configuration management database (CMDB) data not only exacerbates risk but makes it challenging to pass compliance audits.

However, you can gain unparalleled agentless visibility into devices on your network with the ForeScout platform. Deployed as either a physical or virtual solution, this device visibility platform lets you instantly identify devices with IP addresses, including network infrastructure, mobile devices, BYOD systems, non-traditional IoT devices (ATMs, back-office and point-of-sale systems, among others) and rogue endpoints such as unauthorized switches, routers and wireless access points—without requiring management agents or previous device knowledge. Continuous monitoring and assessment identifies new devices, those that enter and leave your network and those that behave as expected.

Securing Access to Financial Networks

Trusted users on your financial networks must have the freedom to access servers and other devices necessary to perform daily tasks. As corporate initiatives increase the demand for technology elasticity, maintaining the speed at which users access their data must be balanced with the need to implement effective network access controls.

The ForeScout platform helps you establish trusted and untrusted zones to protect financial data through network segmentation and network access control. It can automate security segment assignments and create access enforcement using policy-based assignment and enforcement of ACLs and VLANs. The platform enables real-time visibility into devices the minute they connect to the network, to automate and enforce policy-based network access control, endpoint compliance and mobile device security.

Effectively Integrating Your Security Stack

Do your solutions work transparently and effectively together straight out of the box? If you're writing "glue-code" to get point solutions to talk to each other, your technical debt and time to respond to an incident increase, and operational impact can be significant.

The ForeScout platform integrates with more than 70 network security, mobility and IT management products* via ForeScout Extended Modules. This ability to share real-time security intelligence across systems and enforce a unified network security policy increases the speed at which vulnerabilities can be catalogued and their risk levels identified. This reduces vulnerability windows and minimizes operational impact.

FFIEC IT Handbook Security Controls Addressed by the ForeScout Platform

Control #	Title
II.A.2	**Vulnerabilities**
Control Definitions	
Management should assess whether the institution has processes and procedures in place to identify and maintain a catalogue of relevant vulnerabilities, determine which pose a significant risk to the institution, and effectively mitigate and monitor the risks posed by those vulnerabilities.	
ForeScout Solution	
• ForeScout maintains a real-time inventory of every IP-addressable device on the network and, through orchestration using ForeScout Extended Modules, can compare what has been scanned by vulnerability tools and initiate a scan for any missed devices or those that joined the network between scans. • In order to assess which vulnerabilities pose the greatest risk to the business, security and IT staff need to understand what infrastructure supports applications and business processes that are the most critical to the business. At a minimum, this requires an accurate inventory of assets relevant to each application. The ForeScout platform can provide visibility into endpoints on the network, including applications and services running on these endpoints as well as servers which can be synced real time with the CMDB or asset record database. • Measuring the risk represented by a vulnerability requires visibility into mitigating controls to understand exposure. ForeScout can provide visibility into network, infrastructure and endpoint configuration controls to help ensure complete compliance.	
Control #	Title
II.C.4	**Control Implementation**
Control Definitions	
Management should implement controls that align security with the nature of the institution's operations and strategic direction. Based on the institution's risk assessment, the controls should include, but may not be limited to, patch management, asset and configuration management, vulnerability scanning and penetration testing, endpoint security, resilience controls, logging and monitoring...Management should ensure it has the necessary resources, personnel training, and testing to maximize the effectiveness of the controls...The institution can reference one or more recognized technology frameworks and industry standards. Several organizations have published control listings in addition to implementation guidance, including the following: NIST 800 series of publications. These publications provide descriptions of some management processes and technical guidance on many individual controls. **II.C.5. Inventory & Classification of Assets** Management should inventory and classify assets, including hardware, software, information and connections.	
ForeScout Solution	
• The ForeScout platform is a source of truth for real-time asset inventory and intelligence, with productized integration with major vendors such as ServiceNow®. Any asset management program benefits from having an extensible, real-time and accurate platform as a foundation. This includes hardware, infrastructure, software, software versions and more classified by type, vendor and function. • ForeScout provides visibility in real time to endpoint agent-based controls, patching and configuration with orchestration capabilities to remediate automatically or initiate a remediation process. ForeScout complements agent-based security with its agentless approach, which can identify blind spots and gaps in the security posture provided by endpoint protection platforms. • ForeScout's infrastructure-agnostic approach enables real-time visibility into configuration status and gaps for all network infrastructure independent of vendor. • Through extensive partner integrations, ForeScout is able to validate that other security-tool-related processes are complete and compliant with policy, such as vulnerability management, logging and more. • ForeScout gives your team the power of real-time and complete visibility into all control gaps so that the team can spend more time maximizing control design and less time testing and validating control status or responding to incidents as a result of control ineffectiveness. • ForeScout provides real-time visibility into endpoint- and network-based controls in alignment with NIST and other frameworks. NIST 800.53 continuous monitoring is the essence of ForeScout capabiliites. The Forescout Extended Module for Advanced Compliance enables organizations to leverage the SCAP standard to automate configuration and vulnerability assessment and provide security policy compliance metrics and many NIST and CIS Benchmarks.	

Control #	Title
II.C.9 & II.C.9(a)	**Network Controls & Wireless Network Considerations**
Control Definitions	
Management should secure access to computer networks through multiple layers of access controls by doing the following: • Establishing zones (trusted and untrusted) according to the risk profile and criticality of assets contained within the zones and appropriate access requirements within and between each security zone. • Maintaining accurate network diagrams and data flow charts. • Implementing appropriate controls over wired and wireless networks. Policies should prohibit installation of wireless access points and gateways without approval and formal inclusion in the hardware inventory. Network monitoring systems should be configured to detect the addition of new devices. Alternatively, network access control (NAC) systems could prevent the recognition of any unauthorized device…Malicious insiders and attackers may also set up rogue or unauthorized wireless access points and trick employees into connecting. Such access points allow attackers to monitor employee activities. The institution should scan the network regularly to detect rogue access points and consider implementing NAC systems to prevent the successful connection of unauthorized devices…The institution may provide guests with access to a wired or wireless network. The guest network generally is used to provide access to the Internet and should be configured to prevent access to any portion of the production network.	
ForeScout Solution	
Leveraging real-time visibility, ForeScout is able to automate asset inventory reconciliation to ensure an up-to-date and accurate inventory. ForeScout's infrastructure-agnostic and agentless approach enables automated segmentation of network access by user, device classification and/or posture, regardless of how that device is connecting to the network—wired, wireless or VPN. Network segregation strategies can be deployed centrally through the ForeScout platform in order to orchestrate a common strategy across east/west, north/south, campus and data center/cloud vectors.	
Control #	Title
II.C.21	**Business Continuity Considerations**
Control Definitions	
Management should do the following: • Identify personnel who will have critical information security roles during a disaster and train personnel in those roles • Define information security needs for backup sites and alternate communication networks • Establish and maintain policies that address the concepts of information security incident response and resilience, and test information security incident scenarios	
ForeScout Solution	
Planning and implementing a recovery strategy reduces downtime and enables the continuation of vital business and security systems, such as the ForeScout platform. ForeScout supports service resilience, high availability and disaster recovery across its hardware and software components through failover clustering and other options.	

Why ForeScout for FFIEC Compliance?

The ForeScout platform supports and promotes a robust and effective information security program by providing a single-pane-of-glass view of endpoint and network control posture across campus, data center, cloud and OT networks. This capability addresses the need for access control, configuration control and protective control compliance. ForeScout reduces the risk of data breaches and malware attacks by helping to ensure these controls are implemented completely and effectively at all times.

Learn more:

ForeScout Financial Services Solution Brief

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

* As of December 2017

[1] https://www.nist.gov/sites/default/files/documents/2017/02/14/20160219_financial_services_sector_coordinating_council.pdf

[2] https://www.ffiec.gov/about.htm

[3] https://ithandbook.ffiec.gov/media/274793/ffiec_itbooklet_informationsecurity.pdf

[4] https://www.ffiec.gov/cyberassessmenttool.htm

[5] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&