



Business Challenges

- Attestation of NYDFS 500 compliance
- Constant change in regulatory compliance
- Reputational risk resulting from breach disclosure
- Continuous compliance while scaling technology to meet business demands
- Third-party risk management

Technical Challenges

- Asset intelligence of all connected devices, including BYOD, affected by NYDFS 500
- Prevent infected or non-compliant devices from spreading malware
- Measure effectiveness of security controls and demonstrate compliance with NYDFS 500
- Orchestrate unified, automated device remediation and threat response capabilities

Addressing NYDFS Compliance

Build a Resilient Risk Management Program and Comply with NYDFS 500



The ForeScout platform helps you manage risk by providing you with asset intelligence. Amid increased cyberattacks on financial institutions, regulation is evolving and providing even more challenges—both economically and technically. ForeScout helps you reduce risk and helps you improve compliance¹ by providing visibility into all IP-addressable devices connecting to your network(s) while allowing you to automate policies to control access to sensitive data and devices.

Why this regulation?

On March 1, 2017, Title 23 of the New York Codes, Rules and Regulations (NYCRR) Part 500 also known as NYDFS 500, became effective. These minimum cybersecurity standards were warranted given that:

- Threats posed by nation-states, terrorist organizations and independent criminal actors continue to increase
- The financial services industry continues to be a significant target of cybersecurity threats
- Cybercriminals can wreak havoc and cause significant losses for DFS-regulated entities and the consumers they serve

The NYDFS 500 regulation², contained in only 14 pages, is not overly prescriptive, but allows security professionals in financial organizations to assess the company's risk profile and design a program to mitigate these risks. Companies are required to file an annual Certification of Compliance with NYDFS.

Who is affected?

According to Section 500.01, "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law." Person is defined as "any individual or any non-governmental entity, including but not limited to any nongovernmental partnership, corporation, branch, agency or association."

Noteworthy dates: 2018/2019

- February 15th, 2018 – Covered Entities are required to submit the first certification under 23 NYCRR 500.17(b) on or prior to this date.
- March 1st, 2018 – One-year transitional period ends. Covered Entities are required to be in compliance with the requirements of sections 500.04(b), 500.05, 500.09, 500.12 and 500.14(b) of 23 NYCRR Part 500.
- September 3rd, 2018 – Eighteen-month transitional period ends. Covered Entities are required to be in compliance with the requirements of sections 500.06, 500.08, 500.13, 500.14(a) and 500.15 of 23 NYCRR Part 500.
- March 1st, 2019 – Two-year transitional period ends. Covered Entities are required to be in compliance with the requirements of 23 NYCRR 500.11.

Who is not affected?

Section 500.19 exempts companies with a) fewer than 10 employees including contractors; or b) less than \$5 million in gross annual revenue in the last three fiscal years, or c) less than \$10 million in year-end total assets².

Challenges faced by smaller organizations

Section 500.04 of the mandate requires all covered entities to designate a qualified individual to oversee and implement the company's cybersecurity program. Many smaller institutions may choose to hire a third-party service provider to fill this vital Chief Information Security Officer (CISO) role. To be successful, the new CISO must assess risk on an unfamiliar network, yet continuously produce a comprehensive cybersecurity program in time for the annual attestation. ForeScout can help you automate compliance with NYDFS 500 by expertly identifying assets on the network, classifying and assessing device hygiene and helping you identify security gaps.

Steps to Continuous NYDFS 500 Compliance

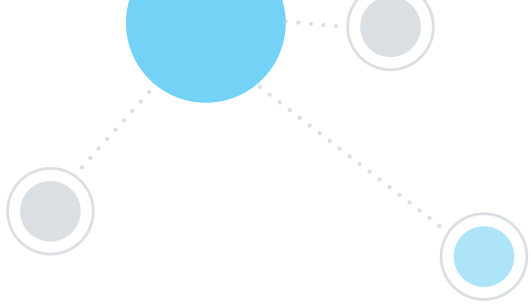
NYDFS 500 mandates compliance reporting via a formal annual attestation and online submission. Covered entities submit their compliance annually via a web portal. Additionally, entities are required to notify the superintendent of cybersecurity within 72 hours from confirmation that a qualifying Cybersecurity Event has occurred.

The NYDFS mandate comprises 24 sections. Sections can be broadly summarized as

- 1.) Continuously conduct full technology risk assessments;
- 2.) Create and maintain an official cybersecurity program, and
- 3.) Ensure cybersecurity policy and procedures are documented, communicated and accessible.

The cybersecurity policy should be based on the organization's risk assessment and address the following areas (Section 500.03 – Cybersecurity Policy) to the extent applicable to the organization's operations:

- (a) information security
- (b) data governance and classification
- (c) asset inventory and device management
- (d) access controls and identity management
- (e) business continuity and disaster recovery planning and resources
- (f) systems operations and availability concerns
- (g) systems and network security
- (h) systems and network monitoring
- (i) systems and application development and quality assurance
- (j) physical security and environmental controls
- (k) customer data privacy
- (l) vendor and third party service provider management
- (m) risk assessment, and
- (n) incident response



What practical steps can you take to ensure that your annual submission goes beyond “paper compliance” and protect your financial networks and systems from a breach?

1. Consider using the FFIEC Cybersecurity Assessment Tool (FFIEC CAT).

The updated FFIEC CAT includes a mapping of the NIST framework to the tool. This mapping helps organizations already using NIST or the FFIEC tool to establish the controls they have in common. This tool can also serve as the basis for complying with NYDFS, since both regulations have similar goals.

2. Conduct a risk assessment of your systems.

Accurate device visibility is foundational to effectively assess risk. The ForeScout device visibility platform provides insight into the diverse types of devices connected to your heterogeneous network—from campus and data center to cloud and operational technology networks, and helps you identify any potential threats that unknown devices may pose to your financial data.

3. Build a resilient cybersecurity program

Discovering devices on your network is just part of the problem that ForeScout can address. Classification is the next important step to keep pace with new devices on your network. Auto-classifying devices is essential for creating effective security policies for network access, device compliance and network segmentation. After discovering and classifying these devices, you can design and build an effective network segmentation program aligned to policies to control access to these segments on a need-to-access basis. Create and maintain a written document containing the policies that you defined.

4. Review the New York State Security Breach Reporting process³

As part of your cybersecurity program, you will need to establish a written incident response plan designed to “promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of [your] Information Systems or the continuing functionality of any aspect of [your] business or operations” (Section 500.16). Further, section 500.17 requires you to notify the superintendent within 72 hours of a determination that a qualifying Cybersecurity event has occurred. ForeScout helps you to tear down security silos and unify infrastructure-wide security management. ForeScout orchestrates formerly disjointed security products allowing them to work as one. This unique set of network, security and management interoperability technologies allows the combined system to let you accelerate response, achieve major operational efficiencies and provide superior security. Quicker response equals quicker notification pursuant to this requirement, if ever there is a breach.

How ForeScout helps with NYDFS 500 compliance



See The ForeScout platform offers the unique ability to see devices the instant they connect to your networks, without requiring software agents or prior knowledge of the device. It sees devices other products simply can't, such as smartphones, tablets, laptops and other corporate-owned and personal mobile devices as well as Internet of Things (IoT) devices, and even detects stealthy sniffer devices that do not utilize an IP address.



Control Unlike systems that flag violations and send alerts to IT and security staff, ForeScout can enforce network access control, endpoint compliance, mobile device security and threat control in one automated system. As a result, financial institutions' employees, contractors and guests can access the appropriate network resources without compromising security. In addition, ForeScout continuously monitors devices on your network and can improve the effectiveness of your security policies so you can demonstrate compliance with the NYDFS 500 regulation.

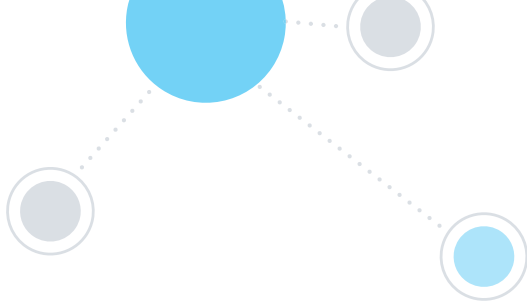


Orchestrate ForeScout integrates with more than 70* network, security, mobility and IT management products. This ability to orchestrate information sharing and operation among myriad security tools allows you to:

- Share context and control intelligence across systems to enforce unified network security policies
- Reduce vulnerability windows by automating system-wide threat response
- Gain higher return on investment (ROI) from your existing security tools while saving time through workflow automation

For a deeper dive into how ForeScout maps to the controls within the NYDFS 500 mandate, see the table below.

NYDFS Section/Sub-section	ForeScout Value
500.02.b.1 - 5 Cybersecurity Program	The ForeScout platform can continuously acquire, assess and take action on new information in order to identify vulnerabilities, remediate non-compliant or compromised devices and minimize the window of opportunity for attackers. The platform can automatically initiate one or more of your policy-based enforcement and remediation actions, ranging from an email notification of non-compliance to mandatory remediation to outright quarantine or access prevention.
500.03.a; 500.03.c - h 500.03.m - Cybersecurity Policy	
500.05.a - b Penetration Testing and Vulnerability Assessments	Comprehensive integration with vulnerability assessment (VA) systems provides the means to initiate scanning of devices and automate policy-based enforcement actions as needed.
500.06.a.2 Audit Trail	When a device requests network access, the ForeScout platform's initial inspection can determine whether logging is enabled and how it is configured, including the chosen location for log storage.
500.07 Access Privileges	The ForeScout platform can identify users attempting to access financial information that are not authorized for such access by their Active Directory group. It provides device and role-based network authentication and authorization, allowing individuals and their devices to get their identified network access determined by VLANs or ACLs.
500.09 Risk Assessment	ForeScout's ability to see and control managed and unmanaged devices, including IoT devices on a network enables you to reduce the risk of potential attacks and remediate issues caused by malicious code or high-risk devices.
500.14.a Training and Monitoring	ForeScout Extended Modules provide true security orchestration between ForeScout and various protection systems. The combined solution can automatically detect indicators of compromise (IOCs) on your financial network(s) and quarantine infected devices, thereby limiting malware propagation and breaking the cyber kill chain.
500.15 Encryption of Nonpublic Information	The ForeScout platform gathers insights regarding the endpoint, its location, who owns it and what's on it. It can help to ensure that encryption and data loss prevention agents are working across the financial network's infrastructure. ForeScout can grant or deny access based on device compliance and user authorization.
500.16 Incident Response Plan	ForeScout Extended Modules for SIEM enable bi-directional integration with leading SIEM systems. With ForeScout and popular SIEM solutions, security teams can: <ul style="list-style-type: none"> • Store ForeScout device visibility data in SIEM solutions for long-term trend analysis, visualization and incident investigation. • Correlate high-value endpoint context from the ForeScout platform with other data sources to identify and prioritize incidents. • Initiate ForeScout control via network and host actions from a SIEM to automate incident response, remediation and threat mitigation. • ForeScout and Splunk customers can leverage the joint solution and Adaptive Response framework within Splunk ES for closed-loop remediation and threat mitigation.
500.17.a.1 - 2 Notices to Superintendent	The ForeScout platform helps satisfy the requirement for notifying the superintendent of cybersecurity within 72 hours from determining that a qualifying cybersecurity event has occurred by helping with incident response through visibility and control of devices on the network and integration with various solutions from Splunk® and ServiceNow®.



Why ForeScout for NYDFS 500 Compliance?

The ForeScout platform helps organizations to build a resilient risk management program by providing visibility into devices within, entering or leaving your network(s); campus to cloud, wired to wireless, IT & OT. The ForeScout platform helps to simplify NYDFS 500 compliance efforts by automating and accelerating device and network control, helping to reduce overall risk and deliver continuous compliance.

ForeScout Technologies is transforming security through visibility, providing Global 2000 enterprises and government agencies with agentless visibility and control of traditional and IoT devices the instant they connect to the network. Our technology continuously assesses, remediates and monitors devices and works with disparate security tools to help accelerate incident response, break down silos, automate workflows and optimize existing investments. As of March 31, 2018, more than 2,800 customers in over 80 countries improve their network security and compliance posture with ForeScout solutions. See devices. Control them. Orchestrate system-wide threat response. **Learn how at www.forescout.com.**

Learn More

[ForeScout Financial Solutions Brief](#)



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 March 31, 2018

¹Securing SWIFT Environments: <https://www.forescout.com/company/resources/seven-steps-securing-swift-environment/>

²<https://www.dfs.ny.gov/legal/regulations/adoptions/gfsrf500.txt>

³<https://its.ny.gov/breach-notification>

© 2018 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners. **Version 06_18**