Silverfort

How to comply with NY-DFS 23 NYCRR Part 500 with Silverfort

Whitepaper

Executive summary

On March 1, 2017, the Department of Financial Services enacted a regulation establishing cybersecurity requirements for financial services companies, 23 NYCRR Part 500 (referred to below as "Part 500" or "the Cybersecurity Regulation").

As a result of investigating hundreds of cybersecurity incidents, Part 500 was amended, increasing the amount and type of security measures organizations are expected to implement to gain sound cyber resilience. **This amendment becomes effective on November 1, 2023.**

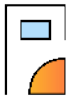
Addressing the identity security aspects of Part 500

The steep rise in the use of compromised credentials for malicious access highlights the importance of protecting the identity attack surface. The amended Part 500 relates to this by requiring comprehensive Multi-Factor Authentication (MFA) and protection for privileged accounts, as well as the implementation of best practices in the monitoring, detection, and response of cyber threats which includes a significant identity protection aspect.

Silverfort Identity Security Platform

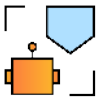
The Silverfort platform integrates with an entity's entire Identity and Access Management (IAM) infrastructure to deliver continuous monitoring, risk analysis, and active enforcement on every authentication and access attempt to any resource. Using these capabilities, Silverfort provides Identity Security Posture Management (ISPM), advanced MFA, service account protection, and Identity Threat Detection and Response (ITDR).

Silverfort for Part 500 protection highlights



Multi-factor authentication

Extend MFA protection to command-line access, legacy apps, IT infrastructure, and other critical resources that couldn't be protected before.



Service account protection

Automate the discovery and monitoring of all service accounts in your environment and enforce auto-created policies to block access if they get compromised.

Securing privileged users

Discover, classify, and enforce least privilege and Just-In-Time (JIT) access policies for all your privileged users.

Detect and respond to identity threats

Detect common credential access, privilege escalation and lateral movement attacks, and respond automatically with real-time blocking.

Mapping Silverfort capabilities to NY-DFS 23 NYCRR Part 500

500.2 Cybersecurity program

(a) Each covered entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the covered entity's information systems and nonpublic information stored on those information systems.

NY-DFS cybersecurity regulation	Silverfort security controls
(b) The cybersecurity program shall be based on the covered entity's risk assessment and designed to perform the following core cybersecurity functions:	**Silverfort continuously monitors the entity's environment to** a) disclose identity-related weaknesses and vulnerabilities and b) detect active identity threats.
(1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of nonpublic information stored on the covered entity's information systems;	The Silverfort platform provides an automated risk analysis of the protected entity's identity attack surface, including DC misconfigurations, insecure authentication protocols, shadow admins, shared users, unchanged passwords, and other weaknesses that increase the entity's exposure to credential access, privilege escalation, or lateral movement.
(2) use defensive infrastructure and the implementation of policies and procedures to protect the covered entity's information systems, and the nonpublic information stored on those information systems, from unauthorized access, use or other malicious acts;	The Silverfort platform enables organizations to configure access policies for both on-prem and cloud environments that enforce alerting, MFA, or access block upon insecure authentication to protected systems.
(3) detect cybersecurity events;	The Silverfort platform includes a risk engine that provides continuous monitoring and risk analysis of every incoming authentication and access attempt. This enables it to detect identity threats, including but not limited to brute force, Pass-the-Hash, Kerberoasting, and access anomalies that indicate malicious presence and activity within the entity's environment.
(4) respond to identified or detected cybersecurity events to mitigate any negative effects;	**Automated response:** the Silverfort platform enables organizations to configure access policies for both on-prem and cloud environments that enforce alerting, request MFA, or block access upon detection of identity threats that were referred to in (3). **Manual response**: the Silverfort platform provides the SecOps team with detailed log screen that includes the full authentication trail of each user, with risk-related filters to expedite and optimize the process of detecting the user accounts that were compromised during the incident. Moreover, the Silverfort platform policies can be hardened to temporarily reduce overall access and harden authentication requirements to block further lateral movement attempts.
(5) recover from cybersecurity events and restore normal operations and services; and	N/A
(6) fulfill applicable regulatory reporting obligations. Design and conduct independent audits of cybersecurity program.	The Silverfort platform enables its users to generate reports periodically or on demand, meeting any auditing requirements that pertain to visibility into user authentication, resource access,and security posture.

500.3 Cybersecurity policy

Each covered entity shall implement and maintain a written policy or policies, approved at least annually by a senior officer or the covered entity's senior governing body for the protection of its information systems and nonpublic information stored on those information systems. Procedures shall be developed, documented and implemented in accordance with the written policy or policies. The cybersecurity policy or policies and procedures shall be based on the covered entity's risk assessment and address, at a minimum, the following areas to the extent applicable to the covered entity's operations:

NY-DFS cybersecurity regulation	Silverfort security controls
(d) access controls, including remote access and identity management;	The Silverfort platform is natively integrated with the Identity and Access Management (IAM) solutions in the entity's environment to gain visibility into and configure access control policies (MFA or access block) for every internal and remote access.

500.7(c) Access privileges

As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.

NY-DFS cybersecurity regulation	Silverfort security controls
(c) Monitor privileged access activity and implement	Silverfort provides organizations with the ability to continuously monitor all privileged access activities and requests for access, enforcing access controls, and ensuring that only authorized users have access to the resources they are entitled to.
(1) a privileged access management solution	Silverfort enables hospitals to easily manage and control privileged accounts by enforcing least privilege and JIT policies that restrict access functions to only what is necessary for each user's role. Through real-time monitoring and automated policy adjustments, Silverfort can automatically discover and classify the number of privileged accounts in use.
(2) *an automated method of blocking commonly used passwords for all accounts on information systems owned or controlled by the class A company and wherever feasible for all other accounts. **The covered entity's CISO may instead approve in writing at least annually the infeasibility and the use of reasonably equivalent or more secure compensating controls*	The Silverfort platform MFA functionality is a reasonably equivalent or more secure compensating control in case the company cannot apply such a solution

500.9 Risk assessment

(a) Each covered entity shall conduct a periodic risk assessment of the covered entity's information systems sufficient to inform the design of the cybersecurity program as required by this Part. Such risk assessment shall be reviewed and updated as reasonably necessary, but at a minimum annually, and whenever a change in the business or technology causes a material change to the covered entity's cyber risk. The covered entity's risk assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the covered entity's business operations related to cybersecurity, nonpublic information collected or stored, information systems utilized and the availability and effectiveness of controls to protect nonpublic information and information systems.

NY-DFS cybersecurity regulation	Silverfort security controls
(b) The risk assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:	
(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the covered entity;	The Silverfort platform assigns a risk score to all user accounts and machines within the entity's environment, as well as authentications involving these entities.
(2) criteria for the assessment of the confidentiality, integrity, security and availability of the covered entity's information systems and nonpublic information, including the adequacy of existing controls in the context of identified risks; and	The Silverfort platform provides a Risk Report functionality that enables organizations to create a summary of the entity's identity security posture in a single click, delivering security teams with clear insights into issues that need resolving.
(3) requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the cybersecurity program will address the risks.	The Silverfort platform provides detailed guidance on the mitigation best practice for every detected risk and the ability to configure an access policy that prevents risky authentications from taking place.

500.12 Multi-Factor Authentication

NY-DFS cybersecurity regulation	Silverfort security controls
(a) Multi-factor authentication shall be utilized for any individual accessing any information systems of a covered entity unless the covered entity qualifies for a limited exemption pursuant to section 500.19(a) of this Part in which case multi-factor authentication shall be utilized for:	The Silverfort platform can enforce MFA protection across all users and resources, on-prem and in the cloud. This applies to all Active Directory authentications, including those that couldn't be protected by MFA before, such as legacy applications, command-line access, databases, networking infrastructure and many others.
(1) remote access to the covered entity's information systems;	The Silverfort platform can enforce MFA protection on all remote access to on-prem and cloud systems
(2) remote access to third-party applications, including but not limited to those that are cloud based, from which nonpublic information is accessible; and	The Silverfort platform can enforce MFA protection on any 3rd party application that is accessed onprem or via cloud directory..
(3) all privileged accounts other than service accounts that prohibit interactive login	The Silverfort platform automatically detects all privileged users and groups, enabling organizations to easily apply MFA protection to all of them. Additionally, the Silverfort platform automates the discovery, monitoring, and protection of service accounts, with auto-generated access policies that trigger either access block or an alert when a service account's behavior deviates from the norm, which could indicate compromise. This allows privileged service accounts to get the same level of protection as other privileged accounts. While section (3) excludes "service accounts that prohibit interactive login" from the MFA requirements, it's important to point that in practice, there is no solution that can prevent a person from performing an interactive login with a service account, thereby voiding the above exclusion. However, using the Silverfort platform's autogenerated policies for service account protection, entities can fully mitigate the scenario in which an adversary attempts to leverage a compromised service account's credentials for malicious access to targeted resources.

500.14(b) Monitoring and training

Each class A company shall implement, unless the CISO has approved in writing the use of reasonably equivalent or more secure compensating controls:

NY-DFS cybersecurity regulation	Silverfort security controls
(1) an endpoint detection and response solution to monitor anomalous activity, including but not limited to lateral movement;	The Silverfort platform monitors all authentications between all endpoints and the other assets of the organization and alerts / deny upon anomalous activity including but not limited to attempts of lateral movement. In addition, Silverfort requires MFA to be performed on every "hop", move between one asset to another, ensuing that stolen credentials cannot be used to progress in the attack path.
(2) a solution that centralizes logging and security event alerting	The Silverfort platform integrates with the customers SIEM system to send its logging and security event alerting for the SOC teams to analyze the information from a centralized system.