New York Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR 500)

strongdm

Simplify and Strengthen NYDFS Compliance with Secure, Centralized Access Management

Frustration-Free Access	Stop Unsanctioned Actions	Continuous Compliance
Enable your team to securely access the resources they need to get the job done without frustration.	Reduce the attack surface and eliminate excess privileges. Continuous detection and mitigation instantly blocks harmful actions.	Policy-based action control ensures real-time, verifiable Zero Trust Compliance.

Simplifying NYDFS Compliance with StrongDM

NYDFS's emphasis on cybersecurity, especially through 23 NYCRR Part 500, has become a model for other regulatory frameworks. With all NYDFS entities being subject to the April 29, 2024 updates, its approach underscores the importance of aligning technological innovation with robust risk management practices, making it an indispensable partner in safeguarding the financial services industry. Colloquially known as NYCRR Part 500, this regulation mandates a comprehensive cybersecurity program, risk assessments, and specific security requirements (like multi-factor authentication [MFA] and safeguards against identity attacks).

StrongDM streamlines NYDFS compliance by centralizing access management, enforcing robust security measures like role-based access control (RBAC), multi-factor authentication (MFA), and end-to-end encryption. It provides comprehensive audit trails, real-time monitoring, and seamless integration with identity providers and SIEM tools to ensure visibility, accountability, and secure operations.

Meet the Updated NYDFS Requirements with StrongDM

StrongDM delivers a **Zero Trust PAM** platform that fulfills the "implementation of a PAM" requirements, while also delivering the critical features required for PoLP, Just-in-Time access, and privileged access. Specifically:

Category	Requirements	How StrongDM Helps
Principle of Least Privilege	(1) limit user access privileges to nonpublic information to only those necessary to perform the user's job; (2) limit the number of privileged accounts and access functions of those accounts to only those necessary to perform the user's job;	(1) StrongDM provides organizations with fine-grained access controls to manage "who has access to what and when" (2) StrongDM centralizes access management to infrastructure, making it possible to easily manage users and the access they possess based on role, attributes and policies
Just-in-Time Access	(3) only permit use of privileged accounts when performing functions requiring that access;	(3) StrongDM makes it possible to enable just-in-time access automating the process of provisioning and deprovisioning credentials. Furthermore, credentials can be revoked at any time or expire based on time, ensuring that privileged access is removed when not in use.
Privileged Access	(4) annually review all user access privileges and remove or disable unnecessary accounts or access; (6) promptly terminate access after departures. Class A: implement a privileged access management solution	(4) StrongDM provides reports that make it easy to understand privilege usage, as well features to disable those privileges where required (6) StrongDM can centrally manage all privileged access to infrastructure, and can be integrated with the organization's identity provider to ensure all privileges are removed across all systems when a user departs Class A: StrongDM qualifies as a privileged access management solution

StrongDM: Zero Trust Privileged Access

StrongDM's Zero Trust PAM provides precise control over privileged actions, enabling secure, on-demand access while minimizing attack surfaces by eliminating excess privileges. With continuous monitoring and instant mitigation, it ensures seamless compliance. It provides:

Real-Time Monitoring and Alerts

Monitor access activity in real-time and receive alerts for unusual or unauthorized behavior.

Granular Role-Based Access Control (RBAC)

Enforce least-privilege principles by assigning precise permissions based on user roles and responsibilities.

Comprehensive Audit Trails

Record every user session, query, and action with full metadata, creating a detailed audit trail for forensic analysis and compliance reporting.

Centralized Access Management

Manage and control access to all critical resources—databases, servers, cloud environments, and more—through a single, unified platform.

Automated Compliance Reporting

Generate on-demand reports with detailed logs of access activity, privileged session management, and security controls.

Risk-Based Access Policies

Configure access policies based on specific risk factors, such as user role, resource sensitivity, or time of access to support risk assessment requirements of NYDFS 23 NYCRR 500.09.