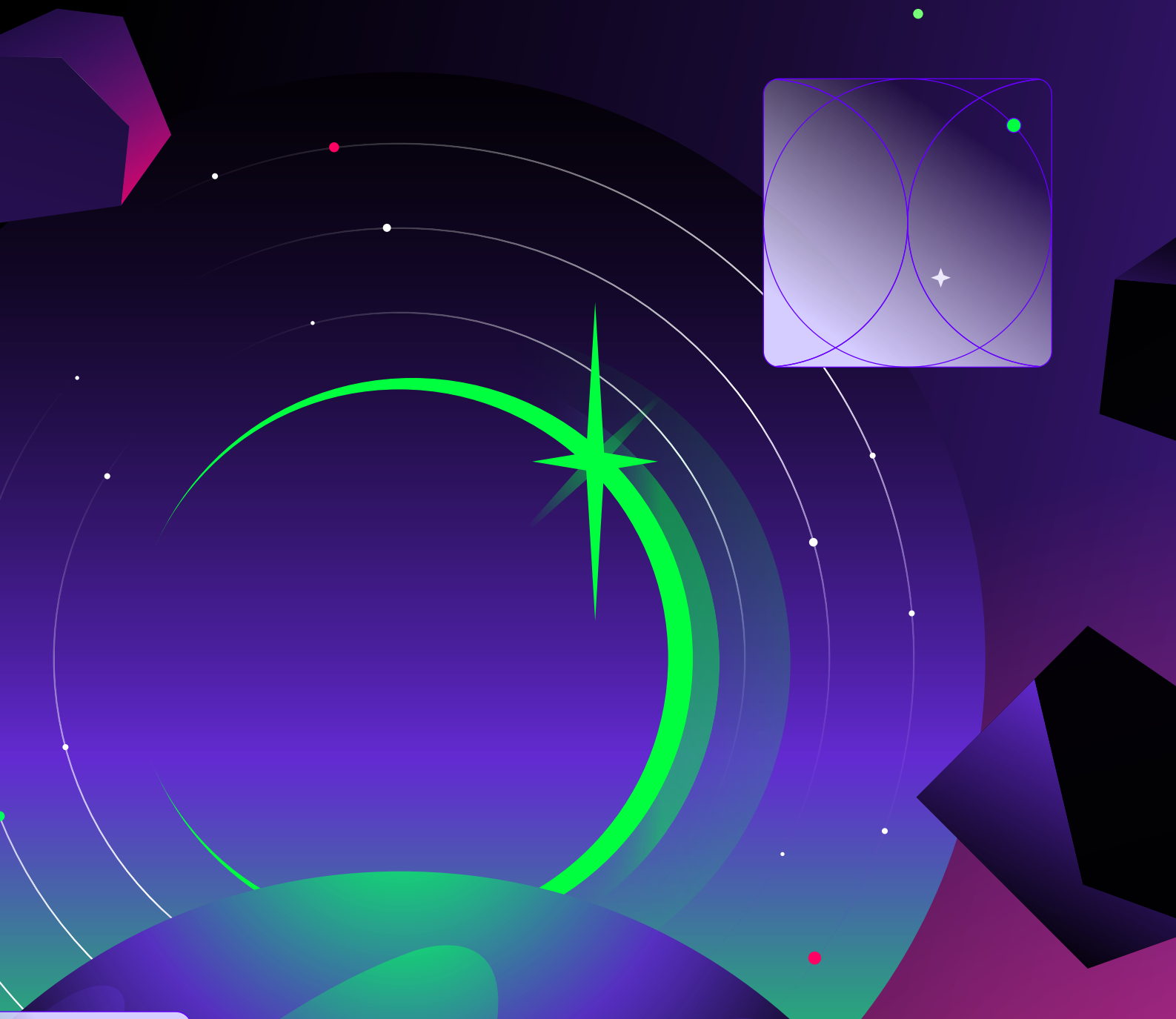
CYERA

WHITEPAPER

NYDFS Part 500's Final Deadline is Approaching

Here's what you need to know, and how Cyera can help



Part 500 in a nutshell

- Enacted on March 1, 2017, 23 NYCRR Part 500 was a landmark cybersecurity
  rule for NY-regulated financial institutions.
- First Amendment (2020): Adjusted administrative/filing requirements and clarified obligations.

Second Amendment (2023): Tightened controls for access, encryption, incident response/BCDR, and governance. Phased in over a two-year period, with the final tranche taking effect November 1, 2025.

What's Due November 1, 2025

NYDFS Requirement	How Cyera Helps
§500.12 — Multi-Factor Authentication (MFA)	
MFA is required for any individual accessing any information system of a covered entity. For smaller entities: • < 20 employees, • < $7.5 million in gross revenue for each of the last three years, OR • < $15 million in total assets MFA is only required for privileged accounts and for remote access to IT systems or third party apps.	Cyera correlates sensitive data to identities so you can scope where MFA must be enforced. It also integrates with identity providers like Okta, and can flag when identities with access to your data, whether internal or external, have not enabled MFA. You can use Cyera's DataPort to publish executive-ready reports on MFA adherence metrics such as which datastores are protected by MFA, and which privileged users have it enabled. Cyera's DataWatcher service will monitor for policy drift (including new users or apps without MFA), raise alerts, and document enforcement for audit purposes. Finally, Cyera's Data Risk Assessment and Breach Readiness services can provide advice and insights on MFA strategy and adoption, helping you ensure MFA is properly scoped.

NYDFS Requirement	How Cyera Helps
§500.13(a) — Asset Inventory (Asset Management & Data Retention)	
Covered entities must produce and maintain a complete, accurate, documented asset inventory of information systems. The asset inventory must track each asset's: • Owner • Location • Classification/sensitivity • Support expiration data • Recovery time objectives • Update/validation frequency	Cyera's agentless DSPM solution periodically scans your data estate across cloud and on-prem resources, allowing it to generate a thorough data asset inventory that includes classification, sensitivity, and ownership context. It also surfaces stale or ghost data, generates alerts, and integrates with other solutions to automate remediation workflows. Omni DLP enforces retention and handling policies based on data classification and sensitivity. DataPort enables GRC and security teams to query your Cyera data, get up-to-date analysis of your data inventory, and maintain a single source of truth for scheduled attestations or validations. Professional services such as DataWatcher allow you to offload monitoring and remediation, and Data Risk Assessment can help you establish an inventory governance cadence and define RTOs. Finally, through its integration with Cohesity, Cyera can help you optimize the frequency of backups based on data criticality and sensitivity.

Past Due Controls (and how Cyera can help you catch up)

NYDFS Requirement	How Cyera Helps
§500.11 — Third-Party Service Provider Security Policy	
Covered entities must perform due diligence, enforce minimum security requirements, and undertake ongoing monitoring of service providers with access to NPI.	Cyera can identify which vendors or SaaS apps have access to NPI. Omni DLP enforces sharing controls and prevents unauthorized transfers. Cyera's AI Guardian identifies AI tools and applications with access to your data, and prevents data leakage by monitoring prompts and blocking exfiltration in AI outputs. Finally, Cyera's Data Risk Assessment and AI Risk Assessment can help identify and document vendor risks to enhance oversight.
§500.15 — Encryption of Nonpublic Information	
Covered entities must maintain a written encryption policy, and encrypt NPI at rest and in transit.	Cyera flags unencrypted datastores and pathways, and Omni DLP protects unencrypted data in transit. DataPort can be used to publish Cyera DSPM's findings, allowing teams to build encryption policy KPIs. Cyera's Data Risk Assessment and AI Risk Assessment services can help your teams perform gap analyses and remediation planning.

NYDFS Requirement	How Cyera Helps
§500.16 — Incident Response Plan (and BCDR)	
Covered entities must maintain an incident response plan that includes performing root-cause analysis, recovery steps, and tabletop testing. The incident response plan must align with the covered entities' business continuity and disaster recovery plans.	By mapping data to identity and sensitivity, Cyera's DSPM can help you establish the likely blast radius of a breach. Omni DLP, AI Runtime Protection, and DataWatcher can detect incidents in near-real time and prevent sensitive data exfiltration. Cyera's Breach Readiness service includes tabletop exercises to test your incident response readiness. Finally, through its integration with Cohesity, Cyera can help you meet your RTOs by identifying sensitive data in backups and prioritizing backup frequency based on data criticality.
§500.17 — Notice of Cybersecurity Incident & Annual Certification	
Covered entities must provide timely notice to NYDFS in the event of a security incident. They must also submit an annual certification of compliance with Part 500.	Cyera helps you establish the blast radius of an incident, logs data events, and can generate reports to support incident documentation. Cyera's DSPM and DataWatcher logs can also be leveraged to support annual certification, while Cyera's Data Risk Assessment and AI Risk Assessment services support your efforts to validate compliance with Part 500.

Fast path to November 2025

- Start where the risk is highest. Use Cyera DSPM to spot your most sensitive systems and privileged access. Turn on MFA there first, then expand.
- Keep a living inventory. With DSPM + DataPort, keep one always-current list of your assets and data. Assign an owner for each item and decide how often you'll review it.
- Connect people to the data they touch. Map sensitive datasets to the humans, apps, and bots that use them. With Omni DLP (and your identity tools), lock things down to least privilege and require MFA for risky actions.
- Let the monitoring run itself. DataWatcher keeps an eye on things 24/7, catches drift, and saves the receipts you'll need for audits.
- Show your work. Use DataPort to package exec-friendly snapshots of MFA coverage, inventory completeness, encryption status, third-party exposure, and incident-response metrics.

SEE HOW CYERA CAN HELP YOU GET READY FOR PART 500'S FULL ROLLOUT.

SCHEDULE A DEMO TODAY AT CYERA.COM.