How Cognito enables compliance with the New York State Department of Financial Services (NYSDFS) Cybersecurity Regulation

Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations establish cybersecurity requirements for financial services companies operating in the state of New York.

The NYSDFS Cybersecurity Regulation, 23 New York Codes, Rules and Regulations (NYCRR) 500, requires New York banks, financial services companies and insurance companies, including non-New York insurance companies who do business in New York, to perform a cybersecurity risk assessment and to create and maintain a cybersecurity program based on the risk assessment.

This risk-based approach is designed to protect the confidentiality, integrity and availability of information systems, ultimately protecting consumers and the New York state financial services industry.

The New York Cybersecurity Regulation by the NYSDFS is meant to address risk to all regulated entities of NYSDFS by outlining a minimum standard. This regulation is aimed at not only protecting customer data, but fortifying information systems that financial organizations use to handle sensitive information.

Since most financial organizations are already required to meet guidelines outlined in the FFIEC, SOX, and the GLBA, the New York Cybersecurity Regulation is generally more prescriptive in nature. It requires institutions to implement specific policies, procedures, and technologies to comply with the regulation.

The NYSDFS Cybersecurity Regulation applies to any business regulated by the NYSDFS under the banking law, insurance law or financial services law. These covered entities include:

- State-chartered banks
- Licensed lenders
- Private bankers
- Service contract providers
- Trust companies
- Mortgage companies
- Foreign banks licensed to operate in New York
- Insurance companies doing business in New York

To help companies comply with the 23 NYCRR 500 financial regulations, the assessment categories supported by the Cognito™ platform from Vectra® are detailed in the following tables.

23 NYCRR 500

Control	Control description	Vectra response
Section 500.02 Cybersecurity Program		
b.1	Identify and assess internal and external cybersecurity risks that may threaten the security or integrity of non-public information stored on the covered entity's information systems.	Automated scoring of hosts reveals the overall risk to the network based on threat and certainty. The Cognito Threat Certainty Index™ scores all threats and prioritizes attacker behaviors and hosts that pose the biggest risk to in-scope assets.
b.3	Detect cybersecurity events	The Cognito platform continuously learns the local environment and tracks all physical and virtual hosts to reveal signs of compromised devices and insider threats. A wide range of cyberthreats are automatically detected in all phases of the attack lifecycle, including: • Command-and-control and other hidden communications • Internal reconnaissance • Lateral movement • Abuse of account credentials • Data exfiltration • Early indicators of ransomware activity • Botnet monetization • Attack campaigns, including the mapping of all hosts and their associated attack indicators The Cognito platform also monitors and detects suspicious access to critical assets by authorized employees, as well as policy violations related to the use of cloud storage, USB storage and other means of moving data out of the network.
Section 500.03 Cybersecurity Policy		
h	Systems and network monitoring	The Cognito platform continuously monitors and analyzes internal network traffic, Internet-bound traffic and data center traffic, including traffic between virtual workloads in the data center, to establish baselines of system behaviors and to identify unapproved activity.
n	Incident response	The Cognito platform enables repeatable incident response and security operations processes by automating manual tasks, including threat detection, event correlation, device triage, and reporting. The highest-risk threats are instantly triaged, correlated to compromised devices and prioritized so security teams can respond faster to stop in-progress attacks and avert data loss. By automating the manual, time-consuming analysis of security events, Cognito condenses weeks or months of work into minutes and reduces the security-analyst workload on threat investigations by 32X.
Section 500.05 Penetration Testing and Vulnerability Assessments		
a	Annual penetration testing of the covered entity's information systems determined each given year based on relevant identified risks in accordance with the risk assessment.	The Cognito platform continuously monitors network traffic to automatically identify hygiene issues that can introduce risk, impair performance or provide opportunities for attackers to hide. Cognito alerts IT security teams about unnoticed errors that may have been introduced during system updates.
Section 500.06 Audit Trail		
a.2	Include audit trails designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operations of the covered entity.	The Cognito platform automatically logs and reports all signs of an attack, including ransomware activity, command-and-control communication, internal reconnaissance, lateral movement, and data exfiltration. Cognito uses rich metadata sources to detect the behaviors exhibited by attackers, the tools used or anomalous events based on deviation from locally learned baselines.

23 NYCRR 500

Control	Control description	Vectra response
Section 500.07 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 non-public information and shall periodically review such access privileges.	The Cognito platform continuously tracks the internal Kerberos infrastructure to understand normal usage in terms of the physical device, user account, and services requested. Kerberos client anomalies can identify when a user's credentials are compromised and when multiple user devices begin sharing access information. In addition, Cognito learns the administrative protocols used on the network, including RDP, SSH, telnet, IPMI, and iDRAC. Cognito also tracks administrator access models for systems, workloads and applications.
Section 500.09 Risk Assessment		
b.2	Criteria for the assessment of the confidentiality, integrity, security and availability of the covered entity's information systems and non-public Information, including the adequacy of existing controls in the context of identified risks.	The Cognito platform continuously monitors network traffic to automatically identify hygiene issues that can introduce risk, impair performance or provide opportunities for attackers to hide. Cognito alerts IT security teams about unnoticed errors that may have been introduced during system updates. In addition, by monitoring attacker behaviors inside the network that occur after the initial infection, Cognito provides awareness of threats that bypass existing malware detection technology.
b.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 Cognito platform automatically identifies anomalies and threats, correlates them to physical host devices, prioritizes the physical host devices with threats that pose the greatest risk, and provides IT security teams with supporting data and recommended next steps. Cognito also allows all host devices in a PCI architecture to be identified and automatically reports all detections on those key assets.
Section 500.10 Cybersecurity Personnel and Intelligence		
a.1	Utilize qualified cybersecurity personnel of the covered entity, an affiliate or a third-party service provider sufficient to manage the covered entity's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in Section 500.02(b)(1)-(6) of this part.	The Cognito platform unburdens and empowers security operations teams that are often understaffed. This is achieved by automating the time-consuming detection and analysis of security events and eliminating the need to endlessly hunt for hidden threats.
a.2	Provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks.	The Cognito platform can serve as a training tool for junior security administrators. It teaches the types of network behaviors related to specific attacks as well as the what an attack lifecycle looks like using real-time network data. Automated detection, triage, and threat prioritization are presented via quick and simple one-page explanations of each attack detection, including possible triggers, root causes, business impacts, and steps to verify.
Section 500.11 Third-Party Service Provider Security Policy		
a.4	Periodic assessment of such third-party service providers based on the risk they present and the continued adequacy of their cybersecurity practices.	The Cognito platform continuously monitors network traffic to automatically identify hygiene issues that can introduce risk, impair performance or provide opportunities for attackers to hide. Cognito alerts IT security teams about unnoticed errors that may have been introduced during system updates.
Section 500.14 Training and Monitoring		
a	Implement risk-based policies, procedures and controls designed to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, non-public information by such authorized users.	*Suspicious administrator behavior*: The Cognito platform identifies misuse of low-level management protocols that control the system below the OS and BIOS, such as IPMI and ILO (HP), and iDRAC (DELL). In addition, Cognito learns the administrative protocols used on the network, including RDP, SSH, and telnet. Cognito also tracks administrator access models for systems, workloads, and applications. *Suspicious Kerberos account*: The Cognito platform identifies when a Kerberos account is being used differently than its learned baseline in one or more ways – connecting to unusual domain controllers, using unusual hosts or accessing unusual services or generating unusual volumes of Kerberos requests using normal domain controllers, usual hosts and usual services.
Section 500.16 Incident Response Plan		
b.1	The internal processes for responding to a cybersecurity event.	The Cognito platform provides automated threat prioritization, allowing for a repeatable, measurable process to detect, triage and report based on continuous monitoring, combined with automated scoring of host devices to reveal the overall risk to the network. Prioritizing threats to the network as they occur enables rapid response by security operations to stop attacks before they cause damage.

Control	Control description	Vectra response
Section 500.17 Notices to Superintendent		
a	Notice of a cybersecurity event. Each covered entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred.	The Cognito platform automated detection, triage and threat prioritization triggers real-time notifications to security teams. Notifications are delivered as one-page explanations of each attack detection, including underlying events and historical context that led to the detection, possible triggers, root causes, business impacts, and steps to verify.

VECTRA®

Security that thinks.®

Email info@vectra.ai **Phone** +1 408-326-2020

vectra.ai