NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

Cybercriminals are exploiting technological vulnerabilities to gain access to sensitive electronic data that can cause severe financial losses for entities regulated by the New York State Department of Financial Services ("NYDFS") and New York consumers. The NYDFS issued 23 NYCRR Part 500 – Cybersecurity Requirements for Financial Services Companies –to ensure that the financial services industry maintains certain minimum cybersecurity standards to protect consumers and ensure that its systems are sufficiently constructed to prevent cyber-attacks to the fullest extent possible. The regulation went into effect on March 1, 2017 with implementation required within 180 days (i.e., by August 28, 2017), and has a number of different compliance deadlines.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
SECTION 500.02: CYBERSECURITY PROGRAM			
(a)	**Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.**	Sophos XG Firewall SG UTM	Enables role-based administration for delegating secure network security management; blocks traffic, services, ports, and protocols except those explicitly allowed and defined as appropriate and necessary for the organization. High availability with active-active load balancing or active-passive fail-over and WAN link balancing ensures availability of critical systems and resources at all times.
		Sophos Intercept X Sophos Intercept X for Server	HIPS, deep learning, anti-exploit, anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host.
		Sophos Mobile	Integration with Sophos UTM, Sophos Wireless access points, and other UTMs provides integrated and consistent security and compliance enforcement for mobile devices accessing the network and other services.
		Sophos Email Appliance	Prevent messages containing sensitive data from leaving the organization with data loss prevention rules providing policy-driven encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to ensure compliance.
		Sophos Phish Threat	Provides simulated phishing cyberattacks and security awareness training for the organizations end users. Courses cover a wide range of topics from phishing and cybersecurity overview lessons through to data loss prevention, password protection and more.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
(b) (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.	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
		All Sophos Products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos Mobile	Monitor mobile devices for jailbreaking and side-loading of applications. Deny access to email, network, and other resources if device is not in compliance with policy.
		Sophos Intercept X for Server	Server Lockdown allows only trusted whitelisted applications and associated files to run.
		Sophos Intercept X Sophos Intercept X for Server	HIPS, deep learning, anti-exploit, anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host.
		Sophos Intercept X Sophos Intercept X for Server	Endpoint Protection application control policies restrict the use of unauthorized applications.
(b) (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.	All Sophos Products	Sophos' user-identity based policy technology allows organizations to enforce role-based user-level controls over network resources and other organization's assets.
		Sophos XG Firewall SG UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group.
		Sophos SafeGuard Encryption	Authenticates users for access to specific protected devices, files, and/or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication.
		Sophos Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
		Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication. Keeps access lists and user privileges information up to date. Provides procedures to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
(b) (3)	**Detect Cybersecurity Events**	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response. All administrative actions are logged and available for reporting and audits.
		Sophos XG Firewall	Controls remote access authentication and user monitoring for remote access, and logs all access attempts.
		Sophos SafeGuard Encryption	Provides detailed logging of all access attempts.
		Sophos Mobile	Creates detailed log events of all malicious activity on managed mobile and traditional endpoints, helping to identify suspicious activity that may try to access sensitive data.
(b) (4)	**Respond to identified or detected Cybersecurity Events to mitigate any negative effects.**	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
		Sophos Email on Central Sophos Email Appliance Sophos XG Firewall SG UTM	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam.
		Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease. Get a root cause analysis of an attack with complete visibility on the how and where of the attack, along with recommendations on what your next steps should be.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
		Sophos XG Firewall	Includes IPS, APT, antivirus, sandboxing with deep learning and web protection to monitor and block malicious, anomalous, and exploitive traffic from in-bound or out-bound access. Sophos Sandstorm, optional cloud-sandbox technology, inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.
(b) (5)	**Recover from Cybersecurity Events and restore normal operations and services.**	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls. The Security Heartbeat also shares this information with Sophos Encryption, which revokes the encryption keys on the affected machine until the problem is fixed to prevent any data theft. After the systems have been automatically returned to their initial, clean state, the XG Firewall restores network access to the device, the encryption keys are returned, and your network is botnet-free.
		Sophos Intercept X Sophos Intercept X for Server	Includes rollback to original files after a ransomware or Master Boot Record attack. Sophos Clean provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware.
(b) (6)	**Fulfill applicable regulatory reporting obligations.**	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response. All administrative actions are logged and available for reporting and audits.
		Sophos XG Firewall	Controls remote access authentication and user monitoring for remote access and logs all access attempts.
		Sophos SafeGuard Encryption	Provides detailed logging of all access attempts.
		Sophos Mobile	Creates detailed log events of all malicious activity on managed mobile and traditional endpoints, helping to identify suspicious activity that may try to access sensitive data.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
SECTION 500.03: CYBERSECURITY POLICY			
(a)	**Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations: Information Security**	Sophos XG Firewall SG UTM Sophos Intercept X Sophos Intercept X for Server	Data Leakage Prevention (DLP) capabilities in Sophos products can detect credit or debit card numbers and prevent leaks of credit and debit card details via email, uploads, and local copying.
		Sophos Email Appliance Sophos XG Firewall SG UTM	Leverages Sophos SPX encryption to dynamically encapsulate email content and attachments into a secure encrypted PDF.
		Sophos Mobile	Sophos Secure Workspace protects work documents with AES-256 encryption, allowing a secure way to manage, distribute, and edit business documents and view web content on mobile devices. Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. Emails and documents can be stored in the secure and encrypted Sophos Container and accessed with the Sophos Secure Email and Sophos Secure Workspace apps.
		Sophos SafeGuard Encryption Sophos Central Device Encryption	Encrypts data on Macs, Windows, and mobile devices. Device Encryption provides centrally-managed, full disk encryption using Windows BitLocker and Mac FileVault. Sophos application-based (synchronized) encryption is automatic and always on, i.e. content is encrypted as soon as it is created and it stays encrypted even when shared or uploaded to a cloud-based file-sharing system or removable devices. Role-based management is available to separate authorization levels and your encryption policies, keys, and self-service key recovery can be centrally managed.
		Sophos Wireless Sophos XG Firewall SG UTM	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos-managed networks and hotspots.
		Sophos XG Firewall SG UTM	Allows for policy-based encryption for VPN tunnels, protecting information in transit.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
(b)	**Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations:** **Data governance and classification**	Sophos Intercept X Sophos Intercept X for Server	Data loss prevention policies prevent misuse and distribution of predefined data sets.
		Sophos Email Appliance Sophos XG Firewall SG UTM	SPX encryption dynamically encapsulates email content and attachments into a secure encrypted PDF to help support compliance.
		Sophos SafeGuard Encryption	A complete data protection solution that is effective across multiple platforms and devices, including mobile and traditional endpoints. Protect data at rest with full disk encryption. Location-based file encryption protects data in motion and follows the file wherever it may go – for example, via email, uploaded to cloud storage, or copied to removable devices. Application-based (synchronized) encryption encrypts data by default as soon as it is created.
		Sophos Mobile	Delivers mobile data protection when integrated with Sophos SafeGuard Enterprise encryption to enable seamless access to encrypted content on mobile devices. The secure Sophos Container for email, documents, and content makes sure that protected data stays separate and can be locked down or wiped.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
(c)	**Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations: Asset inventory and device management**	Sophos XG Firewall SG UTM	Visibility and control over thousands of applications via customizable policy templates with granular controls based on category, risk, technology, or other undesirable characteristics (P2P apps, IMs, games, and other harmful software); fully automated application security with pre-defined policy templates for commonly used enterprise applications/software packages; Synchronized Application Control in XG Firewall identifies all networked applications in the environment running on Sophos-managed endpoints. View a full list of controlled software/applications.
		Sophos Intercept X for Server or Central Server Protection	Discover server instances in AWS or VMs in Azure, and identify if these instances are not protected and which security policies apply.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
(d)	**Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations: Access controls and identity management**	Sophos XG Firewall SG UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group. Sophos XG Firewall with Security Heartbeat™ allows next-generation endpoint and network security to continuously share meaningful information about suspicious events across extended IT ecosystem; detects compromised / unauthorized endpoint devices; allows automated and near instantaneous isolation of the endpoint, preventing it from leaking confidential data.
		Sophos SafeGuard Encryption	Authenticates users for access to specific protected devices, files, and/or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication.
		Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication. Keeps access lists and user privileges information up to date. Provides procedures to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
		Sophos Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
(e)	Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations: Business continuity and disaster recovery planning and resources	Sophos XG Firewall SG UTM	High availability with active-active load balancing or active-passive fail-over and WAN link balancing lets you easily double your performance when you need it.
		Sophos Email on Central	In the event of third-party cloud email service provider outages, alerts are provided if mail can't be delivered to a server/service; email is then queued for delivery to ensures no email is lost, and access to that queued email is provided from a 24/7 emergency inbox inside the end user portal. Retry period for queued email is five days.
		Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls. The Security Heartbeat also shares this information with Sophos Encryption, which revokes the encryption keys on the affected machine until the problem is fixed to prevent any data theft. After the systems have been automatically returned to their initial, clean state, the XG Firewall restores network access to the device, the encryption keys are returned, and your network is botnet-free.
		Sophos Intercept X Sophos Intercept X for Server	Includes rollback to original files after a ransomware or Master Boot Record attack. Sophos Clean provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
(f)	Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations: Systems operations and availability concerns	Sophos XG Firewall SG UTM	High availability with active-active load balancing or active-passive fail-over and WAN link balancing lets you easily double your performance when you need it.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
(g)	**Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations: Systems and network security**	Sophos XG Firewall SG UTM	Enables role-based administration for delegating secure network security management; blocks traffic, services, ports, and protocols except those explicitly allowed and defined as appropriate and necessary for the organization.
		Sophos Mobile	Integration with Sophos UTM, Sophos Wireless access points, and other UTMs provides integrated and consistent security and compliance enforcement for mobile devices accessing the network and other services.
		Sophos Intercept X Sophos Intercept X for Server	HIPS, deep learning, anti-exploit, anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
(h)	**Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations: Systems and network monitoring**	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos XG Firewall SG UTM	iView Reporting provides intelligent, centralized reporting and analytics across multiple firewalls or sites; easy monitoring and analysis of security risks across entire network; convenient backup and long-term storage for security information.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
(i)	**Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations: Systems and application development and quality assurance**	Sophos XG Firewall	Visibility and control over thousands of applications via customizable policy templates with granular controls based on category, risk, technology, or other undesirable characteristics (P2P apps, IMs, games and other harmful software); fully automated application security with pre-defined policy templates for commonly used enterprise applications/software packages; Synchronized Application Control in XG Firewall identifies all networked applications in the environment running on Sophos-managed endpoints. View a full list of controlled software/applications.
		Sophos Mobile	Monitor mobile devices for jailbreaking and side-loading of applications Deny access to email, network, and other resources if device is not in compliance with policy.
		Sophos Intercept X Sophos Intercept X for Server	Endpoint Protection application control policies restrict the use of unauthorized applications.
		Sophos Intercept X for Server	Server Lockdown allows only trusted whitelisted applications and associated files to run.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
(k)	**Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations: Customer data privacy**	Sophos XG Firewall SG UTM Sophos Intercept X Sophos Intercept X for Server	Data Leakage Prevention (DLP) capabilities in Sophos products can detect credit or debit card numbers and can prevent leaks of credit and debit card details via email, uploads, and local copying.
		Sophos Intercept X Sophos Intercept X for Server	Data loss prevention policies prevent misuse and distribution of predefined data sets.
		Sophos SafeGuard Encryption	Complete data protection across multiple platforms and devices, including mobile devices; secures data at rest as well as in transit.
		Sophos Mobile	Delivers mobile data protection when integrated with Sophos SafeGuard Encryption to enable access to encrypted content on mobile devices. The secure Sophos Container for email, documents, and content makes sure that protected data stays separated from personal data and can be locked down or wiped.
		Sophos Email Appliance Sophos XG Firewall SG UTM	SPX encryption dynamically encapsulates email content and attachments into a secure encrypted PDF to help ensure compliance.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
(n)	Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations: Incident response	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
		Sophos Intercept X Sophos Intercept X for Server	Get a root cause analysis of an attack with complete visibility on the how and where of the attack, along with recommendations on what your next steps should be.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
SECTION 500.06: AUDIT TRAIL			
(a) (2)	**(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (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.**	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos XG Firewall SG UTM	iView Reporting provides intelligent, centralized reporting and analytics across multiple firewalls or sites; easy monitoring and analysis of security risks across entire network; convenient backup and long-term storage for security information.
(b)	**Each Covered Entity shall maintain records required by section 500.06(a)(1) of this Part for not fewer than five years and shall maintain records required by section 500.06(a)(2) of this Part for not fewer than three years.**	Sophos XG Firewall SG UTM	iView Reporting provides intelligent, centralized reporting and analytics across multiple firewalls or sites; easy monitoring and analysis of security risks across entire network; convenient backup and long-term storage for security information.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
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.	Sophos XG Firewall SG UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group. Sophos XG Firewall with Security Heartbeat™ allows next-generation endpoint and network security to continuously share meaningful information about suspicious events across extended IT ecosystem; detects compromised / unauthorized endpoint devices; allows automated and near instantaneous isolation of the endpoint, preventing it from leaking confidential data.
		Sophos SafeGuard Encryption	Authenticates users for access to specific protected devices, files, and/or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication.
		Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication. Keeps access lists and user privileges information up to date. Provides procedures to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
		Sophos Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.
SECTION 500.09: RISK ASSESSMENT			
(a)	(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.	All Sophos products	Sophos' user-identity based policy technology allows organizations to enforce role-based user-level controls over network resources and other organization's assets.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
	Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations. 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.	Sophos XG Firewall SG UTM	Visibility and control over thousands of applications via customizable policy templates with granular controls based on category, risk, technology, or other undesirable characteristics (P2P apps, IMs, games, and other harmful software); fully automated application security with pre-defined policy templates for commonly used enterprise applications/software packages.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
(b) (2)	The Risk Assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include: 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;	Sophos Intercept X Sophos Intercept X for Server	Data loss prevention policies prevent misuse and distribution of predefined data sets.
		Sophos XG Firewall SG UTM	Allows policies and security measures to protect information being accessed, processed, or stored at teleworking sites by facilitating two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. High availability with active-active load balancing or active-passive fail-over and WAN link balancing lets you easily double your performance when you need it.
		Sophos SafeGuard Encryption	Supports risk management by authenticating users for access to specific files/folders with the use of user- or group-specific encryption keys.
		Synchronized Security feature in Sophos Products	Enables discovery of unknown cyber risks through identification of all network traffic.
		Sophos Mobile	Provides enterprise mobility and security management capabilities for traditional and mobile endpoints, including security and device policies. Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
(b) (3)	**The Risk Assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include: requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.**	Sophos XG Firewall SG UTM	Includes IPS, APT, antivirus, sandboxing with deep learning, and web protection to monitor and block malicious, anomalous, and exploitive traffic from in-bound or out-bound access. Sophos Sandstorm, optional cloud-sandbox technology, inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.
		Sophos Email Appliance	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam.
		Sophos Mobile	Delivers Unified Endpoint Management (UEM) and security management for traditional and mobile endpoints, helping ensure sensitive data is safe, devices are protected, and users are secure. Sophos Mobile Security provides Mobile Threat Defense for Android and iOS devices, including app, network, and device protection. Leading anti-malware and anti-ransomware protection powered by deep learning for Android devices.
		Sophos Intercept X Sophos Intercept X for Server	HIPS, deep learning, anti-exploit, anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host.
		Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
SECTION 500.10: CYBERSECURITY PERSONNEL AND INTELLIGENCE			
(a) (1)	**Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in section 500.04(a) of this Part, each Covered Entity shall: 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.**	Sophos XG Firewall SG UTM	Enables role-based administration for delegating secure network security management; blocks traffic, services, ports, and protocols except those explicitly allowed and defined as appropriate and necessary for the organization. iView Reporting provides intelligent, centralized reporting and analytics across multiple firewalls or sites; easy monitoring and analysis of security risks across entire network; convenient backup and long-term storage for security information.
		Sophos Mobile	Integration with Sophos UTM, Sophos Wireless access points, and other UTMs provides integrated and consistent security and compliance enforcement for mobile devices accessing the network and other services.
		Sophos Intercept X Sophos Intercept X for Server	HIPS, deep learning, anti-exploit, anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host.
		Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
		All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response. All administrative actions are logged and available for reporting and audits.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
(a) (2)	**Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in section 500.04(a) of this Part, each Covered Entity shall: provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks;**	Sophos Training and Certifications	Training courses and certifications to help partners and customers get the best out of Sophos security deployments; access to latest know-how and expertise for security best practices.
		Sophos Phish Threat	Sophos Phish Threat provides simulated phishing cyber-attacks and security awareness training for the organizations end users. Courses cover a wide range of topics from phishing and cybersecurity overview lessons through to IT training and compliance topics, malware and mobile device risks, password protection, and more.
		SophosLabs	Get the global threat intelligence advantage with our state-of-the-art big data analytics system that efficiently processes millions of emails, URLs, files, and other data points analyzed each day. This data, along with our extensive experience, enables us to develop new definitions, detect entire classes of threats, and even new variants. And, with Live Protection and Live Anti-spam, you benefit from all our data and expert analysis from SophosLabs in real time.
(a) (3)	**Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in section 500.04(a) of this Part, each Covered Entity shall: verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.**	SophosLabs	Get the global threat intelligence advantage with our state-of-the-art big data analytics system that efficiently processes millions of emails, URLs, files, and other data points analyzed each day. This data, along with our extensive experience, enables us to develop new definitions, detect entire classes of threats, and even new variants. And, with Live Protection and Live Anti-spam, you benefit from all our data and expert analysis from SophosLabs in real time.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
SECTION 500.12: MULTI-FACTOR AUTHENTICATION			
(a)	**Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.**	Sophos XG Firewall SG UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group.
		Sophos SafeGuard Encryption	Authenticates users for access to specific protected devices, files, and/or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication.
		Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication. Keeps access lists and user privileges information up to date. Provides procedures to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
		Sophos Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.
		Sophos Email Appliance Sophos XG Firewall SG UTM	Leverages Sophos SPX encryption to dynamically encapsulate email content and attachments into a secure encrypted PDF.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
(b)	**Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.**	Sophos Mobile	Provides enterprise mobility and security management capabilities for traditional and mobile endpoints, including security and device policies. Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. Emails and documents can be stored in the secure and encrypted Sophos Container and accessed with the Sophos Secure Email and Sophos Secure Workspace apps. The Sophos Secure Workspace app secures sensitive data with AES-256 encryption, allowing a secure way to manage, distribute, and edit documents and view web content on mobile devices.
		Sophos XG Firewall SG UTM	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos RED (Remote Ethernet Device) extends a secure network to a remote location easily by establishing a secure, dedicated VPN tunnel.
		Sophos SafeGuard Encryption	Encrypts information at rest and in transit on Macs, Windows, and mobile devices. Manages BitLocker and FileVault full disk encryption as well as always-on file encryption for information stored on hard disks, USB sticks, cloud storage, file shares, memory cards, and CDs/DVDs. All data encrypted remains encrypted as files move across the network.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
SECTION 500.14 TRAINING AND MONITORING			
(a)	**As part of its cybersecurity program, each Covered Entity shall: 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, Nonpublic Information by such Authorized Users; and**	Sophos XG Firewall	Visibility and control over thousands of applications via customizable policy templates with granular controls based on category, risk, technology, or other undesirable characteristics (P2P apps, IMs, games, and other harmful software); fully automated application security with pre-defined policy templates for commonly used enterprise applications/software packages; Synchronized Application Control in XG Firewall identifies all networked applications in the environment running on Sophos-managed endpoints. View a full list of controlled software/applications.
		Sophos Mobile	Monitor mobile devices for jailbreaking and side-loading of applications. Deny access to email, network, and other resources if device is not in compliance with policy.
		Sophos Intercept X	Endpoint Protection application control policies restrict the use of unauthorized applications.
		Sophos Intercept X for Server	Server Lockdown allows only trusted whitelisted applications and associated files to run.
		All Sophos products	Generates security event logs that can be integrated into a centralized monitoring program for incident detection and response.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
(b)	As part of its cybersecurity program, each Covered Entity shall: provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.	Sophos Training and Certifications	Training courses and certifications to help partners and customers get the best out of Sophos security deployments; access to latest know-how and expertise for security best practices.
		Sophos Phish Threat	Sophos Phish Threat provides simulated phishing cyber-attacks and security awareness training for the organizations end users. Courses cover a wide range of topics from phishing and cybersecurity overview lessons through to IT training and compliance topics, malware and mobile device risks, password protection, and more.
		SophosLabs	Get the global threat intelligence advantage with our state-of-the-art big data analytics system that efficiently processes millions of emails, URLs, files, and other data points analyzed each day. This data, along with our extensive experience, enables us to develop new definitions, detect entire classes of threats, and even new variants. And, with Live Protection and Live Anti-spam, you benefit from all our data and expert analysis from SophosLabs in real time.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
SECTION 500.15 ENCRYPTION OF NONPUBLIC INFORMATION			
(a)	As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	Sophos XG Firewall SG UTM Sophos Intercept X Sophos Intercept X for Server	Data Leakage Prevention (DLP) capabilities in Sophos products can detect credit or debit card numbers and can prevent leaks of credit and debit card details via email, uploads, and local copying.
		Sophos Email Appliance Sophos XG Firewall SG UTM	Leverages Sophos SPX encryption to dynamically encapsulate email content and attachments into a secure encrypted PDF.
		Sophos Mobile	Sophos Secure Workspace secures work documents with AES-256 encryption, allowing a secure way to manage, distribute, and edit business documents and view web content on mobile devices. Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. Emails and documents can be stored in the secure and encrypted Sophos Container and accessed with the Sophos Secure Email and Sophos Secure Workspace apps.
		Sophos SafeGuard Encryption Sophos Central Device Encryption	Encrypts data at rest or in transit on Macs, Windows, and mobile devices. Device Encryption provides centrally-managed, full disk encryption using Windows BitLocker and Mac FileVault. Sophos application-based (synchronized) encryption is automatic and always-on, i.e. content is encrypted as soon as it is created and it stays encrypted even when shared or uploaded to a cloud-based file-sharing system or removable devices. Role-based management is available to separate authorization levels and your encryption policies, keys, and self-service key recovery can be centrally managed.
		Sophos Wireless Sophos XG Firewall SG UTM	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos-managed networks and hotspots.

NYDFS Cybersecurity Regulation

(23 NYCRR Part 500)

SOPHOS
Cybersecurity made simple.

SR. NO.	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
		Sophos XG Firewall SG UTM	Allows for policy-based encryption for VPN tunnels, protecting information in transit.
		Sophos Email Appliance	Prevents messages containing sensitive data from leaving the gateway with wizard-based DLP rules or by encrypting them before they leave the network gateway.
SECTION 500.16: INCIDENT RESPONSE PLAN			
(a)	**As part of its cybersecurity program, each Covered Entity shall 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 the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations.**	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
		Sophos Intercept X Sophos Intercept X for Server	Get a root cause analysis of an attack with complete visibility on the how and where of the attack, along with recommendations on what your next steps should be.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2018-12-05 RC (PC)

SOPHOS