NYDFS Cybersecurity Regulation (23 NYCRR Part 500)

On November 1, 2023, the New York Department of Financial Services (NYDFS) finalized updates to its Part 500 – Cybersecurity Requirements for Financial Services Companies – that aims 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. These are the first significant changes to Part 500 since its inception in March 2017.

This latest version went into effect immediately, with some transitional periods when the covered entities must demonstrate compliance with these provisions.

This document describes how Sophos products can be effective tools to help address some of the requirements as part of a customer's efforts to comply with the NYDFS Part 500 cybersecurity regulation.

SOPHOS

Requirement	Sophos solution	How it helps
Section 500.02: 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.	Sophos Firewall	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. Includes IPS, APT, AV, sandboxing with deep learning, and web protection to monitor and block malicious, anomalous, and exploitive traffic from inbound or outbound access. Integration with Sophos MDR and Sophos XDR to provide Automated Threat Response and Synchronized Security to stop threats before they can cause serious problem.
	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 across all devices and platforms.
	Sophos Cloud Optix	Establishes guardrails to prevent, detect, and remediate accidental or malicious changes in network configuration, network traffic, resource configuration, and user behavior or activities.
	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 Mobile	A rich set of device management capabilities keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Flexible compliance rules monitor device health and flag deviation from desired settings.
	Sophos Wireless	Monitors the health status of any Sophos-managed endpoint or mobile device and automatically restricts web access on trusted Wi-Fi networks for those with serious compliance issues. Provides controlled internet access and hotspots for visitors, contractors, and other guests on the network using enterprise-grade backend authentication for a seamless user experience.
	Sophos Managed Detection and Response (MDR)	Threat-hunting experts monitor and correlate signals from across the network, identifying and investigating suspicious activities. Sophos NDR generates high-caliber, actional signals across the network infrastructure to optimize cyber defenses.
	Sophos Rapid Response Service	Get fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
(b) (1) The cybersecurity program shall be based on the covered entity's risk assessment and designed to perform the following core cybersecurity functions: 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.	Sophos XDR	Detect and investigate across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows you to quickly answer business-critical questions, correlate events from different data sources, and take even more informed action.
	Sophos Network Detection and Response (NDR)	Continuously analyzes traffic for suspicious patterns. It detects abnormal traffic flows from unmanaged systems and IoT devices, rogue assets, insider threats, previously unseen zero-day attacks, and unusual patterns deep within the network.
	Synchronized Security feature in Sophos products	Synchronized Security allows Sophos Firewall and Intercept X endpoint protection to work together to identify, isolate and clean up devices that have been compromised, preventing them from leaking confidential data. When the threat is neutralized and there is no risk of lateral movement, network connectivity is restored.
	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. Endpoint Protection application control policies restrict the use of unauthorized applications.

Requirement	Sophos solution	How it helps
	Sophos Managed Detection and Response (MDR)	24/7 monitoring of the environment plus investigation and neutralization of malicious activities secures against data loss through adversarial activities.
	Sophos Cloud Optix	Public cloud security benchmark assessments proactively identify storage services (e.g. Amazon S3), hard drive snapshots, and databases without encryption enabled, or with public access enabled and ports exposed. Guided remediation then instructs the administrator on how to protect these services and data at rest.
(b) (2) The cybersecurity program shall be based on the covered entity's risk assessment and designed to perform the following core cybersecurity functions: 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.	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
	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. Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers. Endpoint Protection application control policies restrict the use of unauthorized applications. Server Lockdown allows only trusted whitelisted applications and associated files to run.
	Synchronized Security feature in Sophos products	Synchronized Security allows Sophos Firewall and Intercept X endpoint protection to work together to identify, isolate and clean up devices that have been compromised, preventing them from leaking confidential data. When the threat is neutralized and there is no risk of lateral movement, network connectivity is restored.
	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	Sophos Cloud Optix	Scans cloud resources for security misconfigurations, profiling any alerts by risk level to help teams focus on the priority areas, and provide detailed remediation guidance to fix those issues.
	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	A rich set of device management capabilities keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Flexible compliance rules monitor device health and flag deviation from desired settings.
	Sophos Firewall	Supports flexible multi-factor authentication options including directory services for access to key system areas. Limits access between untrusted devices and critical servers with segmentation of the internal network and by applying policies, adding a layer of protection and logging to disrupt the attack chain.
	Sophos Managed Detection and Response (MDR)	24/7 monitoring of the environment plus investigation and neutralization of malicious activities secures against data loss through adversarial activities.
	Sophos Network Detection and Response (NDR)	Continuously analyzes traffic for suspicious patterns. It works with your managed endpoints and firewalls to monitor network activity for suspicious and malicious patterns that your endpoints and firewalls cannot see. It detects abnormal traffic flows from unmanaged systems and IoT devices, rogue assets,insider threats, previously unseen zero-day attacks, and unusual patterns deep within the network.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
(b) (3) The cybersecurity program shall be based on the covered entity's risk assessment and designed to perform the following core cybersecurity functions: 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.

Requirement	Sophos solution	How it helps
	Sophos XDR	Detect and investigate across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
	Sophos Firewall	Allows real-time insights into network and user events, quick and easy access to historical data, and easy integration with third-party remote management and monitoring tools (RMMs).
	Sophos Managed Detection and Response (MDR)	Sophos MDR continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events. Anomalous behaviors and code use are detected, investigated and correlated to identify malicious activities and enable us to quickly neutralize the event
	Sophos Network Detection and Response (NDR)	Continuously analyzes traffic for suspicious patterns. It works with your managed endpoints and firewalls to monitor network activity for suspicious and malicious patterns that your endpoints and firewalls cannot see. It detects abnormal traffic flows from unmanaged systems and IoT devices, rogue assets,insider threats, previously unseen zero-day attacks, and unusual patterns deep within the network.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	Sophos Cloud Optix	Enables organizations to design public cloud environments to meet Amazon Web Services, Microsoft Azure, and Google Cloud Platform security best practice standards and maintain them. This agentless service continually monitors public cloud resources, providing the visibility to proactively identify unsanctioned activity, vulnerabilities, and misconfigurations.
(b) (4) The cybersecurity program shall be based on the covered entity's risk assessment and designed to perform the following core cybersecurity functions: 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 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 across all devices and platforms. Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers. Endpoint Protection application control policies restrict the use of unauthorized applications.
	Sophos Firewall	Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Uniquely integrates with Sophos Endpoint, Sophos XDR, and Sophos MDR to automatically respond to any threat or attack identified at the firewall, the endpoint, or by a security analyst. It automatically isolates compromised hosts, preventing lateral movement and external communications until a threat can be investigated and cleaned up.
	Sophos Sandboxing	Complements Sophos web and email security products and Sophos Firewall by inspecting and blocking executables and documents containing executable content before the file is delivered to the user's device.
	Sophos Intercept X for Mobile	Detects malicious and potentially unwanted applications installed on Android devices using Intercept X deep learning technology alongside intelligence from SophosLabs global research team. Integration with Microsoft Intune allows administrators to build conditional access policies, restricting access to applications and data when a threat is detected.
	Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
	Sophos Managed Detection and Response (MDR)	Sophos MDR includes full incident response, delivered by a dedicated team of response specialists who are experts at battling adversaries. Clear procedures and documentation enable consistent info sharing.

Requirement	Sophos solution	How it helps
	Sophos Network Detection and Response (NDR)	When Sophos NDR identifies an indicator of compromise, active threat, or adversary, analysts are immediately alerted and can instantly push a threat feed to Sophos Firewall to trigger an automated response to isolate the compromised host.
	Sophos Rapid Response Service	Get incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
(b) (5) The cybersecurity program shall be based on the covered entity's risk assessment and designed to perform the following core cybersecurity functions: Recover from cybersecurity events and restore normal operations and services.	Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
	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 across all devices and platforms. Includes rollback to original files after a ransomware or master boot record attack. Provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware.
	Sophos Cloud Optix	Scans cloud resources for security misconfigurations, profiling any alerts by risk level to help teams focus on the priority areas, and provide detailed remediation guidance to fix those issues.
	Sophos Firewall	Uniquely integrates with Sophos Endpoint, Sophos XDR, and Sophos MDR to automatically respond to any threat or attack identified at the firewall, the endpoint, or by a security analyst. It automatically isolates compromised hosts, preventing lateral movement and external communications until a threat can be investigated and cleaned up.
	Sophos Managed Detection and Response (MDR)	24/7 threat detection and response identifies and neutralizes advanced cyber attacks that technology alone cannot stop across the full IT environment. Full incident response service included as standard, providing 24/7 coverage delivered by IR experts. Includes full root cause analysis and reporting.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
(b) (6) The cybersecurity program shall be based on the covered entity's risk assessment and designed to perform the following core cybersecurity functions: 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 Cloud Optix	Continuously monitors compliance with custom or out-of-the box templates and audit-ready reports for standards such as PCI DSS, FFIEC, GDPR, HIPAA, and SOC2. Automatically analyzes cloud configuration settings against compliance and security best practice standards without diverting resources. Prevent compliance gaps leaving you exposed with a single view of compliance posture across AWS, Azure, and Google Cloud.
	Sophos Central	Provides flexible reporting tools that allow visualization of network activity and security over time. It offers several built-in compliance reports as well as easy tools to create custom reports.
	Sophos Central Device Encryption	Makes it easy to verify encryption status and demonstrate compliance which is especially useful in cases of lost or stolen devices where organizations must prove that these missing devices are encrypted.

Requirement	Sophos solution	How it helps
Section 500.03: Cybersecurity Policy		
(a) 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 Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
	Synchronized Security feature in Sophos products	Sophos 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 device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.
	Sophos Cloud Optix	Public cloud security benchmark assessments proactively identify shared storage services (e.g. Amazon S3), hard drive snapshots, and databases without encryption enabled, or with public access enabled and ports exposed. Guided remediation then instructs the administrator on how to protect these services and data at rest.
	Sophos Mobile	A rich set of device management capabilities keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Flexible compliance rules monitor device health and flag deviation from desired settings.
	Sophos Managed Detection and Response (MDR)	24/7 monitoring of the environment plus investigation and neutralization of malicious activities secures against data loss through adversarial activities.
	Sophos Firewall	Supports flexible multi-factor authentication options including directory services for access to key system areas. Limits access between untrusted devices and critical servers with segmentation of the internal network and by applying policies, adding a layer of protection and logging to disrupt the attack chain.
(b) 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	SPX encryption dynamically encapsulates email content and attachments into a secure encrypted PDF to help support compliance.
	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	Sophos Mobile	Encrypts documents within a secure container on a mobile device managed with Sophos Mobile. Sophos Secure Workspace can dynamically encrypt content sent to cloud-based storage services and applications. It enforces device encryption and monitors compliance relative to encryption policy.
	Sophos Cloud Optix	Public cloud security benchmark assessments proactively identify shared storage services (e.g. Amazon S3), hard drive snapshots, and databases without encryption enabled, or with public access enabled and ports exposed. Guided remediation then instructs the administrator on how to protect these services and data at rest.
(c) 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 Cloud Optix	Inventory management across multiple-cloud providers with continuous asset monitoring and complete network topology and traffic visualization.

Requirement	Sophos solution	How it helps
	Sophos Intercept X Sophos Intercept X for Server	Device Control allows admins to control the use of removable media through policy settings. Enforces web, data, and device policies to allow only authorized applications to be run, devices to be connected and data to be distributed.
	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.
	Synchronized Security feature in Sophos products	Sophos 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 device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.
(d) 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	All Sophos Products	Sophos' user-identity-based technology powers all policies and reporting across all Sophos products. This allows organizations to enforce role-based user-level controls over network resources and other organizational assets and trace the actions of individual users.
	Sophos Firewall	User awareness across all areas of our firewall governs all firewall policies and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group. Supports flexible multi-factor authentication options including directory services for access to key system areas.
	Sophos Cloud Optix	Connects disparate actions with Sophos AI to identify unusual user access patterns and locations to identify credential misuse or theft. Ensures all identities only perform actions that are required for their tasks and nothing more.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Sophos Mobile	A rich set of device management capabilities keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Flexible compliance rules monitor device health and flag deviation from desired settings.
(e) 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 Managed Detection and Response (MDR)	Sophos MDR detects and investigates suspicious events from across the full security environment to identify threats and appropriate response activities. Data is collected across endpoint, network, identity email, and more, and then correlated using powerful AI tools, threat intelligence and human expertise to identify impact and response.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
	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 across all devices and platforms.
(f) 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 Firewall	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.

Requirement	Sophos solution	How it helps
(g) 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 and monitoring	Sophos Firewall	Includes the latest advanced protection technologies and threat intelligence, such as TLS 1.3 and DPI inspection, machine learning, and cloud sandboxing. Delivers advanced protection from the latest drive-by and targeted web malware, URL/Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection. Sophos Firewall uniquely integrates with Sophos Endpoint, Sophos XDR, and Sophos MDR to automatically respond to any threat or attack identified at the firewall, the endpoint, or by a security analyst. It automatically isolates compromised hosts, preventing lateral movement and external communications until a threat can be investigated and cleaned up.
	Sophos Intercept X Sophos Intercept X for Server	Enforces web, data, and device policies to allow only authorized applications to be run, devices to be connected and data to be distributed.
	Sophos Cloud Optix	Proactively identifies unsanctioned activity, vulnerabilities, and misconfigurations across AWS, Azure, and GCP. Complete cloud edge firewall solution includes IPS, ATP, and URL filtering and lets you deploy several network security products at once to protect your hybrid cloud environments against network threats.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Sophos Managed Detection and Response (MDR)	Threat-hunting experts monitor and correlate signals from across the network, identifying and investigating suspicious activities. Sophos NDR generates high-caliber, actional signals across the network infrastructure to optimize cyber defenses.
	Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
	Sophos Network Detection and Response (NDR)	Continuously analyzes traffic for suspicious patterns. It works with your managed endpoints and firewalls to monitor network activity for suspicious and malicious patterns that your endpoints and firewalls cannot see. It detects abnormal traffic flows from unmanaged systems and IoT devices, rogue assets,insider threats, previously unseen zero-day attacks, and unusual patterns deep within the network.
	Sophos Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos-managed networks and hotspots.
(h) 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: Security awareness and training	Sophos Firewall	Allows real-time insights into network and user events, quick and easy access to historical data, and easy integration with third-party remote management and monitoring tools (RMMs). Uniquely integrates with Sophos Endpoint, Sophos XDR, and Sophos MDR to automatically respond to any threat or attack identified at the firewall, the endpoint, or by a security analyst.
	Sophos Phish Threat	Educates and tests end users against phishing, credential harvesting, or attachment attacks, through automated attack simulations, quality security awareness training, and actionable reporting metrics.
	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.

Requirement	Sophos solution	How it helps
(i) 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 security and development and quality assurance	Cloud Native Security	Enables fast and secure development with integrated security configuration and compliance checks at any stage of the CI/CD pipeline. Works seamlessly with existing DevOps processes to help prevent security breaches pre-deployment. Scans container images in ECR, ACR, Docker Hub registries, as well as GitHub and Bitbucket IaC environments to identify operating system vulnerabilities and fixes to prevent threats pre-deployment. Prevents Infrastructure-as-Code (IaC) templates containing insecure configurations as well as embedded secrets and keys from never making it to a test or live production environment.
	Sophos Factory	Sophos Factory's automation pipelines allow quick introduction of static and dynamic security scanning and testing at any step of the app delivery process. Add security to your existing DevOps workflows by leveraging integrations with GitLab, GitHub, Bitbucket, and other git providers.
(k) 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 Central Device Encryption	Protects devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
	Synchronized Security feature in Sophos products	Sophos 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 device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.
	Sophos Cloud Optix	Public cloud security benchmark assessments proactively identify shared storage services (e.g. Amazon S3), hard drive snapshots, and databases without encryption enabled, or with public access enabled and ports exposed. Guided remediation then instructs the administrator on how to protect these services and data at rest.
	Sophos Mobile	A rich set of device management capabilities keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Flexible compliance rules monitor device health and flag deviation from desired settings.
	Sophos Firewall	Limits access between untrusted devices and critical servers with segmentation of the internal network and by applying policies, adding a layer of protection and logging to disrupt the attack chain. Supports flexible multi-factor authentication options including directory services for access to key system areas.
(l) 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: Vendor and Third Party Service Provider management;	Sophos Intercept X with XDR	Provides comprehensive defense in depth against threats that get in via third party suppliers using AI, exploit prevention, behavioral protection, anti-ransomware and more. Plus, Sophos' XDR functionality enables automatic identification of suspicious activity, prioritizes threat indicators, and quickly searches for potential threats across endpoint and servers.
	Sophos Managed Detection and Response (MDR)	Delivers expert threat hunting and remediation as a fully-managed service. Sophos specialists work around the clock to proactively hunt for, validate, and remediate potential supply chain threats and incidents on your behalf.
	Sophos ZTNA	Helps to safeguard against supply chain attacks that rely on supplier access to your systems via granular access controls. This cloud-delivered solution validates user identity, and device health and compliance before granting access to resources. It authenticates requests from trusted partners, irrespective of the location.

Requirement	Sophos solution	How it helps
(m) 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: Risk assessment	Sophos XDR	Detect and investigate across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
	Sophos Network Detection and Response (NDR)	Includes five independent detection engines that work together in real-time to quickly detect suspicious or malicious traffic and gain critical visibility into network activity that other products can't see.
	Sophos Managed Detection and Response (MDR)	Sophos MDR investigates and assesses potential security risks across the full environment 24/7, leveraging world-leading threat intelligence from Sophos X-Ops to identify risk level and prioritize response. Average time to detect and investigate is just 26 minutes.
(n) 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 and notification	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 Firewall	Uniquely integrates with Sophos Endpoint, Sophos XDR, and Sophos MDR to automatically respond to any threat or attack identified at the firewall, the endpoint, or by a security analyst. It automatically isolates compromised hosts, preventing lateral movement and external communications until a threat can be investigated and cleaned up.
	Sophos Network Detection and Response (NDR)	When Sophos NDR identifies an indicator of compromise, active threat, or adversary, analysts are immediately alerted and can instantly push a threat feed to Sophos Firewall to trigger an automated response to isolate the compromised host.
	Sophos Managed Detection and Response (MDR)	Sophos MDR protection is continually updated using threat intelligence from Sophos X-Ops and real-time data sharing across operators, creating 'community immunity'. Full IR support included, delivered by a team of expert responders.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
(o) 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: Vulnerability Management	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 across all devices and platforms.
	Sophos Firewall	Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Delivers advanced protection from the latest drive-by and targeted web malware, URL/Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
	Sophos XDR	Detects and investigates across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
	Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
	Sophos Managed Detection and Response (MDR)	24/7 detection, investigation and neutralization of suspicious activities by human experts enables us to identify and stop exploitation of vulnerabilities by adversaries. Sophos X-Ops experts keep operators up-to-date on the latest threat and vulnerability developments.

Requirement	Sophos solution	How it helps
Section 500.05: Vulnerability Management		
(a) (1) Each covered entity shall, in accordance with its risk assessment, develop and implement written policies and procedures for vulnerability management that are designed to assess and maintain the effectiveness of its cybersecurity program. These policies and procedures shall be designed to ensure that covered entities: (a) conduct, at a minimum: (1) penetration testing of their information systems from both inside and outside the information systems' boundaries by a qualified internal or external party at least annually;	Sophos Professional Services	Sophos offers vulnerability assessment of security infrastructure and software deployments; and recommendations for architecture and design changes needed to better use the available infrastructure.
(b) Each covered entity shall, in accordance with its risk assessment, develop and implement written policies and procedures for vulnerability management that are designed to assess and maintain the effectiveness of its cybersecurity program. These policies and procedures shall be designed to ensure that covered entities: are promptly informed of new security vulnerabilities by having a monitoring process in place; and	Sophos XDR	Enables rapid detection, investigation, and response to multi-stage threats and active adversaries across your security ecosystem.
	Sophos Managed Detection and Response (MDR)	Continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events.
	Sophos Network Detection and Response (NDR)	Continuously analyzes traffic for suspicious patterns. It works with your managed endpoints and firewalls to monitor network activity for suspicious and malicious patterns that your endpoints and firewalls cannot see. It detects abnormal traffic flows from unmanaged systems and IoT devices, rogue assets, insider threats, previously unseen zero-day attacks, and unusual patterns deep within the network.
	Sophos Cloud Native Security	Cloud Optix allows security teams to focus on and fix their most critical public cloud security vulnerabilities before they are identified and exploited in cyberattacks. By identifying and risk-profiling security, compliance, and cloud spend risks, Cloud Optix enables teams to respond faster, providing contextual alerts that group affected resources with detailed remediation steps.
(c) Each covered entity shall, in accordance with its risk assessment, develop and implement written policies and procedures for vulnerability management that are designed to assess and maintain the effectiveness of its cybersecurity program. These policies and procedures shall be designed to ensure that covered entities: timely remediate vulnerabilities, giving priority to vulnerabilities based on the risk they pose to the covered entity.	Sophos XDR	Automatically prioritizes detections based on risk, providing full context, allowing you to easily identify suspicious activity that needs immediate attention.
	Sophos Cloud Native Security	Allows security teams to focus on and fix their most critical public cloud security vulnerabilities before they are identified and exploited in cyberattacks by identifying and risk-profiling security risks.
	Sophos Managed Detection and Response (MDR)	Sophos MDR investigates and assesses potential security risks across the full environment 24/7, leveraging world-leading threat intelligence from Sophos X-Ops to identify risk levels and prioritize response.
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 Firewall	Allows real-time insights into network and user events, quick and easy access to historical data, and easy integration with third-party remote management and monitoring tools (RMMs).
	Sophos XDR	Automatically prioritizes detections based on risk, providing full context, allowing you to easily identify suspicious activity that needs immediate attention.
	Sophos Managed Detection and Response (MDR)	Sophos MDR detects and investigates suspicious events from across the full security environment to identify threats and appropriate response activities. Data is collected across endpoints, network, identity email, and more, and then correlated using powerful AI tools, threat intelligence and human expertise to identify impact and response.

Requirement	Sophos solution	How it helps
Section 500.07: Access Privileges and Management		
(a) (1) As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall: (1) limit user access privileges to information systems that provide access to nonpublic information to only those necessary to perform the user's job;	Sophos Cloud Optix	Adopt the principle of least privilege across public cloud environments with Sophos Cloud Optix, Cloud Security posture Management solution. The SaaS based service connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real time to identify credential misuse or theft. It includes an IAM visualization tool that provides a complete map of IAM relationships and allows teams to quickly and easily identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks.
	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
	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	Encrypts documents within a secure container on a mobile device managed with Sophos Mobile.. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.
(a)(4) (a) As part of its cybersecurity program, based on the covered entity's risk assessment each covered entity shall: (4) periodically, but at a minimum annually, review all user access privileges and remove or disable accounts and access that are no longer necessary;	Sophos Central	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).
(a)(6) (a) As part of its cybersecurity program, based on the covered entity's risk assessment each covered entity shall: (6) promptly terminate access following departures.	Sophos Central	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).
Section 500.08: Application Security		
(a) Each Covered Entity's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment.	Sophos Cloud Native Security	Enables fast and secure development with integrated security configuration and compliance checks at any stage of the CI/CD pipeline. Works seamlessly with existing DevOps processes to help prevent security breaches pre-deployment. Scans container images in ECR, ACR, Docker Hub registries, as well as GitHub and Bitbucket IaC environments to identify operating system vulnerabilities and fixes to prevent threats pre-deployment. Prevents Infrastructure-as-Code (IaC) templates containing insecure configurations as well as embedded secrets and keys from never making it to a test or live production environment.
	Sophos Factory	Sophos Factory's automation pipelines allow quick introduction of static and dynamic security scanning and testing at any step of the app delivery process. Add security to your existing DevOps workflows by leveraging integrations with GitLab, GitHub, Bitbucket, and other git providers.

Requirement	Sophos solution	How it helps
Section 500.09: 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 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 Intercept X Sophos Intercept X for Server	Consistently looks at reported false positives and false negatives to ensure the product is being continuously improved. It integrates a deep learning malware detection model that can scale to hundreds of millions of training samples and can 'memorize' the entire observable threat landscape as part of its training process. It is regularly trained by our SophosLabs team to stay up to date over time.
	SophosLabs	Delivers the global threat intelligence advantage with Sophos' 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, Live Protection and Live Anti-spam offer the data and expert analysis from SophosLabs in real time.
	Sophos Managed Detection and Response (MDR)	Sophos MDR includes full incident response, delivered by a 24/7 team of response experts. Once an incident is remediated, Sophos MDR performs full root cause analysis which enables the environment to be hardened and response plans and strategies to be updated to incorporate learnings.
Section 500.10: Cybersecurity Personnel and Intelligence		
(a) (1) 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 Managed Detection and Response (MDR)	Sophos MDR detects and investigates suspicious events from across the full security environment to identify threats and appropriate response activities. Data is collected across endpoint, network, identity email, and more, and then correlated using powerful AI tools, threat intelligence and human expertise to identify impact and response.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	Sophos Firewall	Uniquely integrates with Sophos Endpoint, Sophos XDR, and Sophos MDR to automatically respond to any threat or attack identified at the firewall, the endpoint, or by a security analyst. It automatically isolates compromised hosts, preventing lateral movement and external communications until a threat can be investigated and cleaned up.
	Sophos Network Detection and Response (NDR)	Continuously analyzes traffic for suspicious patterns. It works with your managed endpoints and firewalls to monitor network activity for suspicious and malicious patterns that your endpoints and firewalls cannot see. It detects abnormal traffic flows from unmanaged systems and IoT devices, rogue assets,insider threats, previously unseen zero-day attacks, and unusual patterns deep within the network.
(a) (2) 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 XDR	Goes beyond the endpoint, pulling in rich network, email, cloud and mobile data sources to give an even broader picture of the cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.
	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.
	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.

Requirement	Sophos solution	How it helps
Section 500.12: Multi-Factor Authentication		
(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: (1) remote access to the covered entity's information 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 (3) all privileged accounts other than service accounts that prohibit interactive login	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data. It connects users securely to specific applications, not the whole network, from any location. It also includes device health in access policies, ensuring compromised or non-compliant devices are not allowed access to important company data.
	Sophos Firewall	Supports flexible multi-factor authentication options including directory services for access to key system areas. Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
	Sophos Central	Enables protection of privileged and administrator accounts with advanced two-factor authentication.
	Sophos Cloud Optix	Monitors AWS/Azure/GCP accounts for Root user and IAM user access with MFA disabled so you can address and ensure compliance.
Section 500.14 Training and Monitoring		
(a)(1) 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 XDR	Goes beyond the endpoint, pulling in rich network, email, cloud and mobile data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.
	Sophos Network Detection and Response (NDR)	Continuously analyzes traffic for suspicious patterns. It works with your managed endpoints and firewalls to monitor network activity for suspicious and malicious patterns that your endpoints and firewalls cannot see. It detects abnormal traffic flows from unmanaged systems and IoT devices, rogue assets,insider threats, previously unseen zero-day attacks, and unusual patterns deep within the network.
	Synchronized Security feature in Sophos products	Sophos 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 device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.
	Sophos Cloud Optix	Sophos Cloud Optix, Cloud Security Posture Management solution, connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real time to identify credential misuse or theft. It includes an IAM visualization tool that provides a complete map of IAM relationships and allows teams to quickly and easily identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks.
	Sophos Managed Detection and Response (MDR)	Sophos MDR continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events. Anomalous behaviors and code use are detected, investigated and correlated to identify malicious activities and enable us to quickly neutralize the event.
	All Sophos products	Generates security event logs that can be integrated into a centralized monitoring program for incident detection and response.

Requirement	Sophos solution	How it helps
(a)(2) As part of its cybersecurity program, each Covered Entity shall: implement risk-based controls designed to protect against malicious code, including those that monitor and filter web traffic and electronic mail to block malicious content; and	Sophos Firewall	Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Delivers advanced protection from the latest drive-by and targeted web malware, URL/Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
	Sophos Sandboxing	Complements Sophos web and email security products and Sophos Firewall by inspecting and blocking executables and documents containing executable content before the file is delivered to the user's device.
	Sophos Email	Time-of-Click URL rewriting enables analysis of all URLs the moment they are clicked, and allows automatic removal of dangerous emails to protect against these post-delivery techniques. Sophos Email Search and Destroy capabilities take this one step further, directly accessing Office 365 mailboxes, to identify and automatically remove emails containing malicious links and malware at the point the threat state changes and before a user ever clicks on them – removing the threat automatically.
	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 Managed Detection and Response (MDR)	Sophos MDR continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events. Anomalous behaviors and code use are detected, investigated and correlated to identify malicious activities and enable us to quickly neutralize the event.
(a)(3) As part of its cybersecurity program, each Covered Entity shall: provide periodic, but at a minimum annual, cybersecurity awareness training that includes social engineering for all personnel that is updated to reflect risks identified by the covered entity in its risk assessment.	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.
(b)(1) Each class A company shall implement, unless the CISO has approved in writing the use of reasonably equivalent or more secure compensating controls: (1) an endpoint detection and response solution to monitor anomalous activity, including but not limited to lateral movement; and	Sophos Intercept X Endpoint	Takes a comprehensive approach to protecting all endpoints and does not rely on any single security technique. Web, application, and peripheral controls reduce the attack surface and block common attack vectors. AI, behavioral analysis, anti-ransomware, anti-exploitation, and other state-of-the-art technologies stop threats fast before they escalate. Powerful EDR/XDR functionality enables customers to hunt, investigate, and respond to suspicious activity across Sophos and third-party security controls.
(b)(2) Each class A company shall implement, unless the CISO has approved in writing the use of reasonably equivalent or more secure compensating controls: (2) a solution that centralizes logging and security event alerting.	Sophos Central	Offers consolidated views, powerful reporting, and real-time data across cloud, endpoint, and network, delivering actionable insights for faster and more accurate response.
	Sophos XDR	Enables rapid detection, investigation, and response to multi-stage threats and active adversaries across the security ecosystem. Integrates an extensive ecosystem of endpoint, firewall, network, email, identity, and cloud security solutions, including those of third parties, to detect and respond to threats.
	Sophos Managed Detection and Response (MDR)	Sophos MDR continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events. Anomalous behaviors and code use are detected, investigated and correlated to identify malicious activities and enable us to quickly neutralize the event.
	All Sophos products	Generates security event logs that can be integrated into a centralized monitoring program for incident detection and response.

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 Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. For protection of data at rest, Sophos Firewall limits access between untrusted devices and critical servers with segmentation of the internal network and by applying policies, adding a layer of protection and logging to disrupt the attack chain.
	Sophos Email	Automatically scans message bodies and attachments for sensitive data, allowing you to easily establish policies to block or encrypt messages with just a few clicks. Sophos Email Offers TLS encryption and support for SMTP/S along with push-based encryption to send encrypted emails and attachments as password protected documents direct to the user's inbox, full portal-based pull encryption to manage encrypted messages entirely from a secure portal, and S/MIME to encrypt email messages and add a digital signature to safeguard against email spoofing.
	Sophos Mobile	A rich set of device management capabilities keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Flexible compliance rules monitor device health and flag deviation from desired settings.
	Sophos Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.
	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
	Sophos Cloud Optix	Public cloud security benchmark assessments proactively identify shared storage services (e.g. Amazon S3), hard drive snapshots, and databases without encryption enabled, or with public access enabled and ports exposed. Guided remediation then instructs the administrator on how to protect these services and data at rest.

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

2023-12-20 CC (PC)

SOPHOS