NIST Cybersecurity Framework (Version 1.1)

SOPHOS
Cybersecurity made simple.

The U.S. Commerce Department's National Institute of Standards and Technology (NIST) has released version 1.1 of its popular Framework for Improving Critical Infrastructure Cybersecurity, more widely known as the Cybersecurity Framework. The framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. It was developed with a focus on industries vital to national and economic security, including energy, banking, communications, and the defense industrial base. It has since proven flexible enough to be adopted voluntarily by large and small companies and organizations across all industry sectors, as well as by federal, state, and local governments.

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
		IDENTIFY (ID)	
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-2: Software platforms and applications within the organization are inventoried.	**Sophos XG Firewall and 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 .
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	**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

NIST Cybersecurity Framework (Version 1.1)

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	Sophos Endpoint and Server Protection products	Data loss prevention policies prevent misuse and distribution of predefined data sets.
		Sophos Email Appliance Sophos XG Firewall and SG UTM	SPX encryption dynamically encapsulates email content and attachments into a secure encrypted PDF to help support compliance.
		Sophos SafeGuard Encryption	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.

NIST Cybersecurity Framework (Version 1.1)

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
	ID.GV-4: Governance and risk management processes address cybersecurity risks.	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.
		Sophos XG Firewall and 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. Sophos SD-RED [SD-WAN Remote Ethernet Devices] extends a secure network to a remote location easily by establishing a secure, dedicated VPN tunnel.
		Synchronized Security feature in Sophos Products	Enables discovery of unknown cyber risks through identification of all network traffic.
		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.
PROTECT (PR)			
Identity Management, Authentication, and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.	Sophos XG Firewall and 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 device; allows automated and near instantaneous isolation of this 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.

NIST Cybersecurity Framework (Version 1.1)

CATEGORY	SUBCATEGORY	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).
		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.
	PR.AC-3: Remote access is managed.	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 and SG UTM	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos SD-RED [SD-WAN Remote Ethernet Devices] 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.

NIST Cybersecurity Framework (Version 1.1)

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
		Sophos Email Appliance Sophos XG Firewall and SG UTM	Sophos SPX encryption provides 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.
	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	Sophos XG Firewall and 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.

NIST Cybersecurity Framework (Version 1.1)

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
	PR.AC-5: Network integrity is protected (e.g., network segregation, network Segmentation).	Sophos XG Firewall and 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 Endpoint and 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.
	PR.AC.7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	Sophos Enterprise Console and Sophos Central	Configurable role-based administration provides granular control of administrator privileges.
		Sophos Mobile	Role-based administration assures user privacy and appropriate credentials for altering compliance or device/data access.
		Sophos Firewall Manager	Centralized security management with extensive administrative controls; role-based administration with change control and logging.

NIST Cybersecurity Framework (Version 1.1)

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained.	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.
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected.	Sophos XG Firewall and SG UTM Sophos Endpoint and 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 and 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.

NIST Cybersecurity Framework (Version 1.1)

SOPHOS
Cybersecurity made simple.

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
		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.
	PR.DS-2: Data-in-transit is protected.	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 encrypted data remains encrypted as files move across the network.
		Sophos Wireless Sophos XG Firewall and SG UTM	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.
		Sophos XG Firewall and SG UTM	Allows for policy-based encryption for VPN tunnels, protecting information in transit.
		Sophos Email Appliance Sophos XG Firewall and SG UTM	Sophos SPX encryption provides 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.

NIST Cybersecurity Framework (Version 1.1)

SOPHOS
Cybersecurity made simple.

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
	PR.DS-4: Adequate capacity to ensure availability is maintained.	Sophos XG Firewall and 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.
	PR.DS-5: Protections against data leaks are implemented.	Sophos Endpoint and 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 and SG UTM	SPX encryption dynamically encapsulates email content and attachments into a secure encrypted PDF to help ensure compliance.
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	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.

NIST Cybersecurity Framework (Version 1.1)

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
		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 Endpoint and 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.
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-3: Configuration change control processes are in place.	All Sophos products	All administrative actions are logged and available for reporting and audits.
	PR.IP.7: Protection processes are Improved.	Sophos Intercept X and Sophos Intercept X for Server	Intercept X continuously 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.

NIST Cybersecurity Framework (Version 1.1)

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	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 5 days.
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	Sophos Central	Keeps access lists and user privileges information up to date. Procedures are in place 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).
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	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.

NIST Cybersecurity Framework (Version 1.1)

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
	PR.PT-2: Removable media is protected and its use restricted according to policy.	**Sophos Endpoint and Intercept X for Server products**	Device Control allows admins to control the use of removable media through policy settings.
		Sophos SafeGuard Encryption	Provides complete data protection across multiple platforms and devices, including mobile devices; secures data at rest as well as in transit.
		Sophos Mobile	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.
	PR.PT-4: Communications and control networks are protected.	**Sophos Email Appliance**	Sophos SPX encryption provides 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 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 SafeGuard Encryption	Encrypts data on Macs, Windows, and mobile devices. Manages BitLocker and FileVault full disk encryption as well as always-on file encryption 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.
	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	**Sophos XG Firewall and 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.

NIST Cybersecurity Framework (Version 1.1)

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
		DETECT (DE)	
Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-2: Detected events are analyzed to understand attack targets and methods.	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos Intercept X and Sophos Intercept X for Server	Get the 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.
		Sophos Intercept X for Server	Prevent unauthorized applications from running with Server Protection, automatically scanning your system for known good applications, and whitelisting only those applications.
		Sophos XG Firewall and SG UTM	iView Reporting offers 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.
	DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos XG Firewall and 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.

NIST Cybersecurity Framework (Version 1.1)

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
	DE.AE-4: Impact of events is determined.	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 and 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.
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events.	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos XG Firewall and 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.
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos XG Firewall and SG UTM	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.

NIST Cybersecurity Framework (Version 1.1)

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
	DE.CM-5: Unauthorized mobile code is Detected.	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 Endpoint Protection Advanced	Endpoint Protection application control policies restrict the use of unauthorized applications.
		Sophos Server Protection	Server Lockdown allows only trusted whitelisted applications and associated files to run.
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	All Sophos products	Generates security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		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.

NIST Cybersecurity Framework (Version 1.1)

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-5: Detection processes are continuously improved.	Sophos Intercept X and Sophos Intercept X for Server	Intercept X 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.
		RESPOND (RS)	
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	RS.RP-1: Response plan is executed during or after an incident.	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 and 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.
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-2: Incidents are reported consistent with established criteria.	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos XG Firewall and 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.

NIST Cybersecurity Framework (Version 1.1)

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
	RS.CO-3: Information is shared consistent with response plans.	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos XG Firewall and 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.
Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated.	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 and SG UTM	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.
		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 and 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.

NIST Cybersecurity Framework (Version 1.1)

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
	RS.AN-3: Forensics are Performed.	Sophos Intercept X and 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.
	RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers).	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 and 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.
		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.
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	RS.MI-1: Incidents are contained.	Sophos Intercept X and Sophos Intercept X for Server	Anti-exploit, anti-ransomware, and deep learning malware detection protect endpoints from malicious executable code.
		Sophos Intercept X and 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.
		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.

NIST Cybersecurity Framework (Version 1.1)

CATEGORY	SUBCATEGORY	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.
		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.
		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.
	RS.MI-2: Incidents are mitigated.	Sophos Intercept X and Intercept X for Server	Anti-exploit, anti-ransomware, and deep learning malware detection protect endpoints from malicious executable code.
		Sophos Intercept X and 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.
		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.

NIST Cybersecurity Framework (Version 1.1)

CATEGORY	SUBCATEGORY	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.
		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.
		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.
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	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.
		SophosLabs	Sophos' state-of-the-art big data analytics system 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.

NIST Cybersecurity Framework (Version 1.1)

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. .	RS.IM-1: Response plans incorporate lessons learned.	Sophos Intercept X and Sophos Intercept X for Server	Intercept X continuously 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.
	RS.IM-2: Response strategies are updated.	Sophos Intercept X and Sophos Intercept X for Server	Intercept X 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.
		RECOVER (RC)	
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident.	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 and Intercept X for Server	Includes rollback to original files after a ransomware or Master Boot Record attack, along with Sophos Clean which provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware as well.

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

2020-04-13 RC-NA [MP]

SOPHOS