NIST Cybersecurity Framework (Version 1.1)

SOPHOS

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. This document maps out how Sophos solutions offer effective tools to help address some of the requirements as part of a customer's efforts to comply with the NIST CSF.

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 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 Sophos Firewall identifies all networked applications in the environment running on Sophos Managed Endpoints.
		Sophos Cloud Optix	Inventory management across multiple-cloud providers with continuous asset monitoring and complete network topology and traffic visualization.
		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 Intercept X for Server	Does not permit unauthorized applications from running, automatically scanning your system for known good applications, and whitelisting only those applications.
		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.
	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.
		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, powerful XDR functionality enables you to automatically identify suspicious activity, prioritize threat indicators, and quickly search for potential threats across your endpoint and servers.
		Sophos ZTNA	Safeguards against supply chain attacks that rely on supplier access to your systems via very 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.

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 Intercept X Sophos Intercept X for Server	Data loss prevention policies prevent misuse and distribution of predefined data sets.
		Sophos Email Sophos Firewall	Granular control of data breach prevention policies, including multi-rule policies for groups and individual users with seamless integration of encryption. Create custom CCLs using Sophos Content Control Lists or customize out of the box templates for specific CCLs. Choose from a variety of policy outcomes including block, drop attachment, quarantine as well as log and continue mode.
		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 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.
	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 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 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.
		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	HIPS, Deep Learning, Anti-exploit, Anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host.
		Sophos Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos-managed networks and hotspots.
		Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
Risk Assessment (ID. RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	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 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.

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
	ID.RA-6: Risk responses are identified and prioritized	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 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
		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	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.
Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and cyber supply chain risk management plan.	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, powerful XDR functionality enables you to automatically identify suspicious activity, prioritize threat indicators, and quickly search for potential threats across your 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	Safeguards against supply chain attacks that rely on supplier access to your systems via very 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.
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.	All Sophos products	Sophos' user-identity based policy technology allows user level controls over network resources and other organization's assets.
		Sophos Firewall	User awareness across all areas of our firewall governs all firewall policies and reporting, giving user-level controls over applications, bandwidth, and other network resources.
		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).
		Sophos ZTNA	Enables better security and more agility in quickly changing environments by making it quick and easy to enroll or decommission users and devices. Continuously validates user identity, device health, and compliance before granting access to applications and data.

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
	PR.AC-3: Remote access is managed.	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. Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
		Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
		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.
		Sophos Email	Delivers granular control of data breach prevention policies, including multi-rule policies for groups and individual users with seamless integration of encryption. Create custom CCLs using Sophos Content Control Lists or customize out of the box templates for specific CCLs. Choose from a variety of policy outcomes including block, drop attachment, quarantine as well as log and continue mode.
	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	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 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 Switch	Allows network access control that enables you to authenticate users using LDAP, MAC address, or other authentication methods to connect to a network. This prevents unauthenticated users and devices from gaining access to your LAN.
		Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
		Sophos Central	Configurable role-based administration provides granular control of administrator privileges. Keeps access lists and user privileges information up to date. Protects privileged and administrator accounts with advanced two-factor authentication.
		Sophos Central	Does not permit shared administrator accounts. Each employee has his or her own account, with explicit permissions granted to each account. Protects privileged and administrator accounts with advanced two-factor authentication.

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
	PR.AC-5: Network integrity is protected (e.g., network segregation, network Segmentation).	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. Supports flexible multi-factor authentication options including directory services for access to key system areas. Flexible and powerful segmentation options via zones and VLANs provide ways to separate levels of trust on your network while enabling added protection against lateral movement between different parts of your network.
		Sophos Switch	Allows configuration of VLANs to segment your internal traffic and reduce the attack surface in case of an infection or breach. Allows network access control that enables you to authenticate users using LDAP, MAC address, or other authentication methods to connect to a network. This prevents unauthenticated users and devices from gaining access to your LAN.
		Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	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 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 ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
		Sophos Central	Protects 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.
		Sophos Switch	Allows network access control that enables you to authenticate users using LDAP, MAC address, or other authentication methods to connect to a network. This prevents unauthenticated users and devices from gaining access to your LAN.
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	Educates and tests end users against phishing, credential harvesting, or attachment attacks, through automated attack simulations, quality security awareness training, and actionable reporting metrics.

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
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 Firewall Sophos Intercept X Sophos Intercept X for Server	Data Leakage Prevention (DLP) capabilities in Sophos products can detect sensitive data like credit or debit card numbers and can prevent leaks of such information via email, uploads, and local copying.
		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.
		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 Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
		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.
	PR.DS-2: Data-in-transit is protected.	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
		Sophos Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos-managed networks and hotspots.
		Sophos Firewall	Allows for policy-based encryption for VPN tunnels, protecting data in transit
		Sophos Email	Granular control of data breach prevention policies, including multi-rule policies for groups and individual users with seamless integration of encryption. Create custom CCLs using Sophos Content Control Lists or customize out of the box templates for specific CCLs. Choose from a variety of policy outcomes including block, drop attachment, quarantine as well as log and continue mode.
		Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
	PR.DS-4: Adequate capacity to ensure availability is maintained.	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.

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
	PR.DS-5: Protections against data leaks are implemented.	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)	24/7 monitoring of the environment plus investigation and neutralization of malicious activities secures against data loss through adversarial activities.
		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	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 Email	SPX encryption dynamically encapsulates email content and attachments into a secure encrypted PDF to help ensure compliance.
		Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
		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 Firewall	Limits access between untrusted devices and critical servers with the segmentation of the internal network and by applying policies, adding a layer of protection and logging to disrupt the attack chain. Lateral Movement Protection, a Synchronized Security feature, prevents the threat or hacker from spreading to other systems, stealing data, or communicating back to the host.
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	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 ZTNA	Validates user identity, device health, and compliance before granting access to resources.
		Sophos Mobile	Monitor mobile devices for jailbreaking and side-loading of applications Deny access to email, network, and other resources if device is not in compliance with policy.
		Sophos Intercept X Sophos Intercept X for Server	Endpoint protection application control policies restrict the use of unauthorized applications.
		Sophos Switch	Allows network access control that enables you to authenticate users using LDAP, MAC address, or other authentication methods to connect to a network. This prevents unauthenticated users and devices from gaining access to your LAN.
		Sophos Email Sophos Firewall	Offers TLS encryption and support for SMTP/S along with full push-base, and optional pull-based portal encryption.
		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.

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
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-4: Backups of information are conducted, maintained, and tested periodically.	Sophos Cloud Optix	Monitors AWS, Azure and GCP accounts for cloud storage services without backup schedules enabled and provides guided remediation.
	PR.IP-7: Protection processes are Improved.	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 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.
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recoveryand Disaster Recovery) are in place and managed.	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.
	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).

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
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.
		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 Mobile	Creates detailed log events of all malicious activity on mobile devices, 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 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.
	PR.PT-2: Removable media is protected and its use restricted according to policy.	Sophos Intercept X Sophos Intercept X for Server	Device Control allows admins to control the use of removable media through policy settings.
	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality.	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.
	PR.PT-4: Communications and control networks are protected.	Sophos Email	Sophos Email Content Control allows customers to filter inbound and outbound messages for keywords and file types – Identifying specific keywords in email subject lines, message content, and file names. The content inspection capabilities will recursively unpack archives so that the contained files are inspected independently. The solution is able to identify PDF using their true file-type and set policy around those file types. 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 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. Supports flexible multi-factor authentication options including directory services for access to key system areas.
	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	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.

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 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 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 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.
	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 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 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.
	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 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.

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
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 Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
		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 Email Sophos Firewall	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam.
		Sophos 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 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 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 Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	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 Central	Does not permit shared administrator accounts. Each employee has his or her own account, with explicit permissions granted to each account. Protects privileged and administrator accounts with advanced two-factor authentication.
		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	Continuously validates user identity, device health, and compliance before granting access to applications and data.
		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

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
	DE.CM-4: Malicious code is detected.	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 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	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
		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 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 Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	DE.CM-5: Unauthorized mobile code is Detected.	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 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 Intercept X Sophos Intercept X for Server	Endpoint Protection application control policies restrict the use of unauthorized applications.
		Sophos Intercept X for Server	Server Lockdown allows only trusted whitelisted applications and associated files to run.
		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.
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
		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.

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
	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.
		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 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.
		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 Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
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 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)	Via the Sophos Adaptive Cybersecurity Ecosystem, which underpins all our defenses, detection processes are continually enhanced.
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 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.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
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 Managed Detection and Response (MDR)	Provides human-led response to active threats with direct customer communication via both email and phone.
	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 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.

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
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.
		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 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 Managed Detection and Response (MDR)	Sophos MDR investigates suspicious signals, correlating data and behaviors and leveraging Sophos X-Ops threat intelligence for context and insights. On notification of vulnerabilities, Sophos MDR proactively hunts for exposure to enable swift remediation.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	RS.AN-3: Forensics are Performed.	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 Managed Detection and Response (MDR)	Sophos MDR investigates suspicious signals, correlating data and behaviors and leveraging Sophos X-Ops threat intelligence for context and insights. On notification of vulnerabilities, Sophos MDR proactively hunts for exposure to enable swift remediation.
	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 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 Managed Detection and Response (MDR)	Sophos MDR investigates suspicious signals, correlating data and behaviors and leveraging Sophos X-Ops threat intelligence for context and insights. On notification of vulnerabilities, Sophos MDR proactively hunts for exposure to enable swift remediation.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
		SophosLabs	Provides 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 the development of 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.

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
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 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	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
		Sophos Email Sophos Firewall	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam.
		Sophos Intercept X 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 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.
		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 Managed Detection and Response (MDR)	Sophos MDR swiftly contains and neutralizes incidents, with average time to detect, investigate and respond to just 38 minutes. Clients choose the level of response they wish us to take.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	RS.MI-2: Incidents are mitigated.	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	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
		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 Managed Detection and Response (MDR)	Sophos MDR swiftly contains and neutralizes incidents, with average time to detect, investigate and respond to just 38 minutes. Clients choose the level of response they wish us to take.
		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	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.

CATEGORY	SUBCATEGORY	SOPHOS SOLUTION	HOW IT HELPS
	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.
		Sophos Managed Detection and Response (MDR)	Sophos MDR swiftly contains and neutralizes incidents, with average time to detect, investigate and respond to just 38 minutes. Clients choose the level of response they wish us to take.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
		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.
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 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)	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.
	RS.IM-2: Response strategies are updated.	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.
		Sophos Managed Detection and Response (MDR)	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.
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 Sophos Firewall restores network access to the device, the encryption keys are returned, and your network is botnet-free.
		Sophos Managed Detection and Response (MDR)	Sophos MDR includes full incident response, delivered by a 24/7 team of response experts.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.

2022-11-16 (NP)

SOPHOS