Sarbanes-Oxley (SOX) Act Compliance Reference Card

SOPHOS

The Sarbanes-Oxley Act of 2002, also known as the Public Company Accounting Reform and Investor Protection Act, was enacted in response to a number of major corporate and accounting scandals. The Act, commonly referred to by the acronym "SOX," led to a series of regulations imposing strict rules and accountability regarding reporting and record-keeping requirements for all publicly traded companies in order to protect investors and the public from fraudulent accounting practices.

The SOX legislation does not mandate a control framework for use towards compliance; instead, it requires organization to adopt a recognized control framework. COBIT is a widely recognized and accepted framework supporting IT-specific efforts towards complying with SOX sections 302 and 404. The following table lists some of the key provisions of the COBIT framework and explains how Sophos can help your organization implement these provisions and achieve compliance with SOX.

Specifications and descriptions are subject to change without notice. Sophos disclaims all warranties and guarantees regarding this information. Use of Sophos products alone does not guarantee legal compliance. The information in this document does not constitute legal advice. Customers are solely responsible for compliance with all laws and regulations, and should consult their own legal counsel for advice regarding such compliance.

CONTROL DESCRIPTION	SOPHOS SOLUTION	HOW IT HELPS
AP007.06 Manage contract staff Ensure that consultants and contract personnel who support the enterprise with I&T skills know and comply with the organization's policies and meet agreed contractual requirements.	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 Firewall	Allows user awareness across all areas of our firewall governs all firewall policies and reporting, enabling user-level control over applications, bandwidth and other network resources.
	Sophos ZTNA	Safeguards contract staff 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.
	Sophos Central	Keeps access lists and user privileges information up-to-date. Procedures are in place to revoke access rights if individuals no longer meet the conditions to receive access.
	Sophos Cloud Optix	Enables adoption of 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 possible credential misuse or theft. 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.

APO10.04 Manage vendor risk Identify and manage risk relating to vendors' ability to continually provide secure, efficient and effective service delivery. This also includes the subcontractors or upstream vendors that are relevant in the service delivery of the direct vendor.	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.
APO12.01 Collect data. Identify and collect relevant data to enable effective I&T-related risk identification, analysis and reporting.	Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
	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.
APO12.06 Respond to risk. Respond in a timely manner to materialized risk events with effective measures to limit the magnitude of loss.	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)	24/7 detection, investigation, and neutralization of suspicious activities by human experts enables us to identify and stop exploitation of vulnerabilities by adversaries. 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.

APO13.01 Establish and maintain an information security management system (ISMS). Establish and maintain an information security management system (ISMS) that provides a standard, formal and continuous approach to information security management, enabling secure technology and business processes that are aligned with business requirements.	Sophos Firewall	Enables role-based administration for delegating secure network security management; blocks traffic, services, ports and protocols except those explicitly allowed and defined as appropriate and necessary for the organization. Includes IPS, APT, AV, sandboxing with deep learning, and web protection to monitor and block malicious, anomalous, and exploitive traffic from inbound or outbound access. 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 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	ECloud Optix enables organizations to design public cloud environments to meet Amazon Web Services, Microsoft Azure, and Google Cloud Platform security best practice standards and maintain them. This agentless service continually monitors public cloud resources, providing the visibility to proactively identify unsanctioned activity, vulnerabilities, and misconfigurations. ‣ Comprehensive asset inventory and network visualizations of security groups, cloud workloads, share storage, databases, IAM roles and more ‣ Automatic identification of security best practice and compliance gaps leaving organizations exposed, with guided remediation. ‣ Continuously monitor compliance with custom or out-of-the box templates and audit-ready reports for standards such as FFIEC, GDPR, HIPAA, PCI DSS, and SOC2. ‣ Integrate security in the DevOps CI/CD pipeline to scan container images and infrastructure-as-code templates and more to block vulnerabilities pre-deployment.
	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 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.
	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 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 enables enforcement of device encryption and monitors compliance relative to encryption policy.
	Sophos Wireless	Offers visibility into wireless networks health and clients connecting to the network. With visibility into potential threats, such as rogue APs, insight into clients with compliance or connectivity issues and advanced diagnostics, identifying and troubleshooting issues is quick and easy.
	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.

APO13.03 Monitor and review the information security management system (ISMS). Maintain and regularly communicate the need for, and benefits of, continuous improvement in information security. Collect and analyse data about the information security management system (ISMS), and improve its effectiveness. Correct nonconformities to prevent recurrence.	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.
APO14.03 Establish the processes and infrastructure for metadata management. Establish the processes and infrastructure for specifying and extending metadata about the organization's data assets, fostering and supporting data sharing, ensuring compliant use of data, improving responsiveness to business changes and reducing data-related risk	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 cleanup 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 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 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	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 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 Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.
	Sophos Firewall	Limits access between untrusted devices and critical servers with segmentation of the internal network and by applying policies, adding a layer of protection and logging to disrupt the attack chain. 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.
APO14.09 Support data archiving and retention. Ensure that data maintenance satisfies organizational and regulatory requirements for availability of historical data. Ensure that legal and regulatory requirements for data archiving and retention are met.	Sophos Cloud Optix	Cloud Optix identifies where backups are not being taken within public cloud infrastructure accounts and alerts the security team within the Cloud Optix console to take action. Continuously monitor compliance with custom or out-of-the box templates and audit-ready reports for standards such as FFIEC, GDPR, HIPAA, PCI DSS, and SOC2. Automatically analyze cloud configuration settings against compliance and security best practice standards without diverting resources. Prevent compliance gaps leaving you exposed with a single view of compliance posture across AWS, Azure, and Google Cloud.

AAPO14.10 Manage data backup and restore arrangements. Manage availability of critical data to ensure operational continuity.	Sophos Cloud Optix	Monitors AWS, Azure and GCP accounts for cloud storage services without backup schedules enabled and provides guided remediation.
BAI08.02 Organize and contextualize information into knowledge Organize information based on classification criteria. Identify and create meaningful relationships among information elements and enable use of information. Identify owners, and leverage and implement enterprise-defined information levels of access to management information and knowledge resources	Sophos Firewall	Allows user awareness across all areas of Sophos firewall governs all firewall polices and reporting, enabling user-level control over applications, bandwidth and other network resources.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	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 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 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 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 enables enforcement of device encryption and monitors compliance relative to encryption policy.
DSS01.03 Monitor I&T infrastructure. Monitor the I&T infrastructure and related events. Store sufficient chronological information in operations logs to reconstruct and review time sequences of operations and other activities surrounding or supporting operations.	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
	Sophos Firewall	Allows real-time insights into network and user events, quick and easy access to historical data, and easy integration with third-party remote management and monitoring tools (RMMs).
	Sophos XDR	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 Cloud Optix	Cloud Optix enables organizations to design public cloud environments to meet Amazon Web Services, Microsoft Azure, and Google Cloud Platform security best practice standards and maintain them. This agentless service continually monitors public cloud resources, providing the visibility to proactively identify unsanctioned activity, vulnerabilities, and misconfigurations.

DSS02.02 Record, classify and prioritize requests and incidents. Identify, record and classify service requests and incidents and assign a priority according to business criticality and service agreements.	Sophos Cloud Optix	Scans cloud resources for security misconfigurations, profiling any alerts by risk level to help teams focus on the priority areas, and provide detailed remediation guidance to fix those issues.
	Sophos 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.
DSS02.04 Investigate, diagnose and allocate incidents. Identify and record incident symptoms, determine possible causes, and allocate for resolution.	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 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. 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.
DSS02.05 Resolve and recover from incidents. Document, apply and test the identified solutions or workarounds. Perform recovery actions to restore the I&T-related service.	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.
	Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
	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.
DSS02.07 Track status and produce reports. Regularly track, analyze and report incidents and fulfilment of requests. Examine trends to provide information for continual improvement.	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. Full root cause analysis by Sophos MDR enables the environment to be hardened and response plans and strategies to be updated to incorporate learnings.
	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.

DSS03.05 Perform proactive problem management. Collect and analyze operational data (especially incident and change records) to identify emerging trends that may indicate problems. Log problem records to enable assessment.	Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
	Sophos Intercept X Sophos Intercept X with XDR 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. 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 Firewall	Allows real-time insights into network and user events, quick and easy access to historical data, and easy integration with third-party remote management and monitoring tools (RMMs).
	Sophos Managed Detection and Response (MDR)	Sophos MDR 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.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	Sophos Cloud Optix	Enables organizations to design public cloud environments to meet Amazon Web Services, Microsoft Azure, and Google Cloud Platform security best practice standards and maintain them. This agentless service continually monitors public cloud resources, providing the visibility to proactively identify unsanctioned activity, vulnerabilities, and misconfigurations. ‣ Comprehensive asset inventory and network visualizations of security groups, cloud workloads, share storage, databases, IAM roles and more ‣ Automatic identification of security best practice and compliance gaps leaving organizations exposed, with guided remediation. ‣ Continuously monitor compliance with custom or out-of-the box templates and audit-ready reports for standards such as FFIEC, GDPR, HIPAA, PCI DSS, and SOC2. ‣ Integrate security in the DevOps CI/CD pipeline to scan container images and infrastructure-as-code templates and more to block vulnerabilities pre-deployment.
DSS04.07 Manage backup arrangements. Maintain availability of business-critical information.	Sophos Cloud Optix	Cloud Optix identifies where backups are not being taken within public cloud infrastructure accounts and alerts the security team within the Cloud Optix console to take action.

DSS05.01 Protect against malicious software. Implement and maintain preventive, detective and corrective measures (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malicious software (e.g., ransomware, malware, viruses, worms, spyware, spam).	Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms. Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers. Endpoint Protection application control policies restrict the use of unauthorized applications.
	Sophos Firewall	Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. 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 Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
	Sophos Managed Detection and Response (MDR)	24/7 detection, investigation and neutralization of suspicious activities by human experts enables us to identify and stop exploitation of vulnerabilities by adversaries. Sophos X-Ops experts keep operators up-to-date on the latest threat and vulnerability developments.
	Sophos Rapid Response Service	Get incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
DSS05.02 Manage network and connectivity security. Use security measures and related management procedures to protect information over all methods of connectivity.	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 Managed Detection and Response (MDR)	Threat hunting experts monitor and correlate signals from across the network, identifying and investigating suspicious activities. Sophos NDR generates high caliber, actional signals across the network infrastructure to optimize cyber defenses.
	Sophos Email	Automatically scans message bodies and attachments for sensitive data, allowing you to easily establish policies to block or encrypt messages with just a few clicks. Sophos Email Offers TLS encryption and support for SMTP/S along with push-based encryption to send encrypted emails and attachments as password protected documents direct to the user's inbox, full portal-based pull encryption to manage encrypted messages entirely from a secure portal, and S/MIME to encrypt email messages and add a digital signature to safeguard against email spoofing.
	Sophos 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.
	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 Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.

DSS05.03 Manage endpoint security. Ensure that endpoints (e.g., laptop, desktop, server, and other mobile and network devices or software) are secured at a level that is equal to or greater than the defined security requirements for the information processed, stored or transmitted.	Sophos Intercept X Sophos Intercept X for Server Sophos Intercept X for Mobile	Works across all your desktops, laptops, servers, tablets, and mobile devices and across all major operating systems to protect all endpoints. HIPS, Deep Learning, Anti-exploit, Anti-adversary, and malicious traffic detection in Sophos Intercept X combine to proactively detect malicious behaviors occurring on the host.
	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
	Synchronized Security feature in Sophos products	Sophos Firewall with Security Heartbeat™ allows next-generation endpoint and network security to continuously share meaningful information about suspicious events across extended IT ecosystem; detects compromised / unauthorized endpoint device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.
	Sophos Managed Detection and Response (MDR)	24/7 monitoring of the environment plus investigation and neutralization of malicious activities on endpoints secures against data loss through adversarial activities.
	Sophos Cloud Optix	Public cloud security benchmark assessments proactively identify shared storage services (e.g. Amazon S3), hard drive snapshots, and databases without encryption enabled, or with public access enabled and ports exposed. Guided remediation then instructs the administrator on how to protect these services and data at rest.
	Sophos Mobile	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 Firewall	Limits access between untrusted devices and critical servers with segmentation of the internal network and by applying policies, adding a layer of protection and logging to disrupt the attack chain. 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.
DSS05.04 Manage user identity and logical access. Ensure that all users have information access rights in accordance with business requirements. Coordinate with business units that manage their own access rights within business processes.	All Sophos Products	**Use identity-based access:** Sophos' user-identity based policy technology allows organizations to enforce role-based user-level controls over network resources and other organization's assets.
	Sophos Firewall	**Access controls:** Allows user awareness across all areas of our firewall governs all firewall polices and reporting, enabling user-level control 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 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.

DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events. Using a portfolio of tools and technologies (e.g., intrusion detection tools), manage vulnerabilities and monitor the infrastructure for unauthorized access. Ensure that security tools, technologies and detection are integrated with general event monitoring and incident management.	Sophos Firewall	Includes IPS, APT, antivirus, sandboxing with deep learning, and web protection to monitor and block malicious, anomalous, and exploitive traffic from inbound or outbound access.
	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 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.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Sophos 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.
	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 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.
DSS06.03 Manage roles, responsibilities, access privileges and levels of authority. Manage business roles, responsibilities, levels of authority and segregation of duties needed to support the business process objectives. Authorize access to all information assets related to business information processes, including those under the custody of the business, IT and third parties. This ensures that the business knows where the data are and who is handling data on its behalf.	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 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 Central	Protects privileged and administrator accounts with advanced two-factor authentication. Keeps access lists and user privileges information up to date.
	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
	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	User awareness across all areas of our firewall governs all firewall polices and reporting, giving user-level controls over applications, bandwidth and other network resources. Allows for granular rule-based traffic control to specific ports and services at perimeter ingress and egress points, and can control remote access authentication and user monitoring at the perimeter.
	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.

DSS06.06 Secure information assets. Secure information assets accessible by the business through approved methods, including information in electronic form (e.g., portable media devices, user applications and storage devices, or other methods that create new assets in any form), information in physical form (e.g., source documents or output reports) and information during transit. This benefits the business by providing end-to-end safeguarding of information.	Sophos Cloud Optix	Public cloud security benchmark assessments proactively identify shared storage services (e.g. Amazon S3), hard drive snapshots, and databases without encryption enabled, or with public access enabled and ports exposed. Guided remediation then instructs the administrator on how to protect these services and data at rest.
	Sophos Intercept X Sophos Intercept X for Server	Device Control allows admins to control the use of removable media through policy settings.
	Sophos Managed Detection and Response (MDR)	24/7 monitoring of the environment plus investigation and neutralization of malicious activities secures against data loss through adversarial activities.
	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS.
	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 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 Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.
MEA03: Managed Compliance with External Requirements Evaluate that I&T processes and I&T-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with; integrate IT compliance with overall enterprise compliance. Ensure that the enterprise is compliant with all applicable external requirements.	Sophos Cloud Optix	Continuously monitor compliance with custom or out-of-the box templates and audit-ready reports for standards such as FFIEC, GDPR, HIPAA, PCI DSS, and SOC2. Automatically analyze cloud configuration settings against compliance and security best practice standards without diverting resources. Prevent compliance gaps leaving you exposed with a single view of compliance posture across AWS, Azure, and Google Cloud.

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

Oxford, UK

2022-11-23 RC-NA (MP)

SOPHOS