# ISO/IEC 27001:2022

ISO 27001 is an international standard published by the International Standardization Organization (ISO), and it describes how to manage information security in a company. It was written by the world's best experts in the field of information security and provides a methodology for the implementation of information security management in an organization. The focus of ISO 27001 is to protect the confidentiality, integrity, and availability of information in a company. On October 25, 2022, ISO 27001:2022 was released, replacing the version from 2013. The standard can be implemented in any kind of organization, profit or non-profit, private or state-owned, small or large.

**Note**: ISO/IEC 27001 is split into 11 sections, plus Annex A. Sections 0 to 3 are introductory, describing the standard, and are not mandatory for organizations to implement. Sections 4 to 10 set the requirement for an information security system and must be implemented by an organization if it wants to be compliant with the standard. Many of these sections highlight policies, planning, and procedures at the organizational level - which are outside of the scope of this document. This document discusses Annex A, which contains 93 security controls or safeguards grouped into 4 domains: Organizational, People, Physical, and Technical. The document maps out how Sophos solutions can support organizations to meet the security controls in Annex A. This is not a replacement for ISO 27001. To get the standard, visit the ISO website: http://www.iso.org.



SOPHOS

# ISO 27001:2022 – Annex A security controls

| Control | Description | Sophos solution | How it helps |
|---|---|---|---|
| **A.5 Organizational Controls** | | | |
| **A 5.2: Information Security Roles and Responsibilities** | Information security roles and responsibilities shall be defined and allocated according to the organization's needs. | All Sophos Products | Sophos' user-identity-based technology allows organizations to enforce role-based user-level controls over network resources and other organizational assets. |
| **A 5.3: Segregation of duties** | Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. | All Sophos products | Sophos' user-identity-based technology allows user-level controls over network resources and other organizational assets. |
| | | Sophos Central | Does not permit shared administrator accounts. Each employee has his or her own account, with explicit permissions granted to each account.<br>Protects privileged and administrator accounts with advanced two-factor authentication. |
| **A 5.7: Threat Intelligence** | Information relating to information security threats shall be collected and analysed to produce threat intelligence. | Sophos XDR | Pulls in rich network, endpoint, 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. |
| | | 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 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. |
| **A 5.11: Return of Assets** | Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement. | 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. |
| **A 5.15: Access Control** | Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements. | Sophos Firewall | Supports flexible multi-factor authentication options including directory services for access to key system areas. |
| | | Sophos Cloud Optix | Adopt the principle of least privilege across public cloud environments with Sophos Cloud Optix, Cloud Security Posture Management solution.<br>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.<br>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 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. |

| Control | Description | Sophos solution | How it helps |
|---|---|---|---|
| **A 5.16: Identity Management** | The full life cycle of identities shall be managed. | Sophos Firewall<br>Sophos Central | 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.<br>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). |
| **A 5.18: Access Rights** | Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control. | Sophos Firewall | User awareness across all areas of Sophos firewall governs all firewall policies 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.<br>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. |
| | | Sophos Intercept X<br>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 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). |
| **A 5.19: Information Security in Supplier Relationships** | Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services. | 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. |
| **A 5.20: Addressing Information Security Within Supplier Agreements** | Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship. | 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. |
| **A 5.26: Response to Information Security Incidents** | Information security incidents shall be responded to in accordance with the documented procedures. | 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. |
| | | 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. |

| Control | Description | Sophos solution | How it helps |
|---|---|---|---|
| | | Sophos Intercept X<br>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.<br>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. |
| **A 5.27: Learning from Information Security Incidents** | Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls. | Sophos Managed Detection and Response (MDR) | Sophos MDR proactively responds to vulnerability disclosure by the client. On notification, a full investigation is initiated that looks for signs of exploitation. If necessary, Sophos MDR will remediate the incident and provide guidance on how to harden the environment against future exploitation. |
| | | Sophos Intercept X<br>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. |
| **A 5.28: Collection of Evidence** | The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events. | All Sophos products | Generated security event logs can be integrated into a centralized monitoring program for incident detection and response. |
| | | Sophos XDR | Pulls in rich network, endpoint, 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. |
| **A 5.29: Information Security During Disruption** | The organization shall plan how to maintain information security at an appropriate level during disruption. | 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. |
| **A 5.32: Intellectual Property Rights** | The organization shall implement appropriate procedures to protect intellectual property rights. | Sophos Firewall<br>Sophos Intercept X<br>Sophos Intercept X for Server | Data Leakage Prevention (DLP) capabilities in Sophos products can detect sensitive data and can prevent leaks of such information via email, uploads, and local copying. |
| | | 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 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.<br>Flexible compliance rules monitor device health and flag deviation from desired settings. |
| | | 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 ZTNA | Validates user identity, device health, and compliance before granting access to resources. |

| Control | Description | Sophos solution | How it helps |
|---|---|---|---|
| | | Sophos Central Device Encryption | Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance. |
| **A 5.33: Protection of Records** | Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release. | Sophos Email | Prevent data loss by creating multi-rule DLP policies for groups and individual users to ensure the protection of sensitive information with discovery of confidential contents in all emails and attachments. |
| | | Sophos Firewall<br>Sophos Intercept X<br>Sophos Intercept X for Server | Data Leakage Prevention (DLP) capabilities in Sophos products can detect sensitive data and can prevent leaks of such information via email, uploads, and local copying. |
| | | 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 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.<br>Flexible compliance rules monitor device health and flag deviation from desired settings. |
| | | 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 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. Verify device encryption status and demonstrate compliance. |
| **A 5.34: Privacy and Protection of Personal Identifiable Information (PII)** | The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements. | Sophos Email | Prevent data loss by creating multi-rule DLP policies for groups and individual users to ensure the protection of sensitive information with discovery of confidential contents in all emails and attachments. |
| | | Sophos Firewall<br>Sophos Intercept X<br>Sophos Intercept X for Server | Data Leakage Prevention (DLP) capabilities in Sophos products can detect sensitive data and can prevent leaks of such information via email, uploads, and local copying. |
| | | 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. Verify device encryption status and demonstrate compliance. |
| **A 5.36: Compliance with Policies, Rules and Standards for Information Security** | Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed. | Sophos Cloud Optix | Automatically maps security and compliance standards to your environments and offers on-demand audit-ready reports that detail where organizations pass or fail the requirements of each standard, with the option to include remediation steps within the reports themselves. |

| Control | Description | Sophos solution | How it helps |
|---|---|---|---|
| **A.6 People Controls** | | | |
| **A 6.3: Information Security Awareness, Education and Training** | Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function. | Sophos Training and Certifications | Training courses and certifications to help users get the best out of Sophos security deployments; access to latest know-how and expertise for security best practices. |
| | | Sophos Phish Threat | Provides simulated phishing cyberattacks and security awareness training for the organization's end users. Courses cover a wide range of topics from phishing and cybersecurity overview lessons, through to data loss prevention, password protection and more. |
| **A 6.7: Remote Working** | Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises. | Sophos Firewall | Initiates interactive remote access connection while ensuring that the cyber asset is not accessed directly by providing additional factors for security using MFA and OTP.<br>Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.<br>Controls remote access authentication and user monitoring for remote access and logs all access attempts. |
| | | Sophos ZTNA | Continuously validates user identity, device health, and compliance before granting access to applications and data. It authenticates requests for access from trusted users, irrespective of the location. |
| | | Synchronized Security feature in Sophos products | Provides granular configuration to ensure only healthy managed devices can access applicable cyber assets. |
| | | 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.<br>Flexible compliance rules monitor device health and flag deviation from desired settings. |
| | | 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 neutralize the event quickly. |
| **A.7 Physical Controls** | | | |
| **A 7.9: Security of Assets Off-Premises** | Off-site assets shall be protected. | Sophos Mobile | Provides Enterprise Mobility and security management capabilities for mobile devices, including security and device policies. Flexible compliance rules monitor device health and flag deviation from desired settings. |
| | | 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.<br>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 Intercept X<br>Sophos Intercept X for Server | Scans web content and allows category-based web filtering to be enforced both on and off the corporate network. |
| **A.8 Technological Controls** | | | |
| **A 8.1: User Endpoint Devices** | Information stored on, processed by or accessible via user end point devices shall be protected. | Sophos Intercept X<br>Sophos Intercept X for Server | Protection for all endpoints – Windows, Mac, Linux, and virtual machines – integrated with 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.<br>Get a root cause analysis of an attack with complete visibility on the how and where of the attack, along with recommendations on what your next steps should be. |

| Control | Description | Sophos solution | How it helps |
|---|---|---|---|
| | | Synchronized Security feature in Sophos products | Synchronized Security allows Sophos Firewall and Intercept X endpoint protection to work together to identify, isolate and clean up devices that have been compromised, preventing them from leaking confidential data. When the threat is neutralized and there is no risk of lateral movement, network connectivity is restored. |
| | | Sophos Central Device Encryption | Enables protection of devices and data with full disk encryption for Windows and macOS. |
| | | Sophos Managed Detection and Response (MDR) | Sophos MDR continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events. Anomalous behaviors and code use are detected, investigated, and correlated to identify malicious activities and enable us to quickly neutralize the event. |
| **A 8.2: Privileged Access Rights** | The allocation and use of privileged access rights shall be restricted and managed. | 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.<br>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 | 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). |
| **A 8.3: Information Access Restriction** | Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control. | 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.<br>Supports flexible multi-factor authentication options including directory services for access to key system areas. |
| | | 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. |
| | | 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.<br>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 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.<br>Flexible compliance rules monitor device health and flag deviation from desired settings. |
| **A 8.5: Secure Authentication** | Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control. | Sophos Central | Configurable role-based administration provides granular control of administrator privileges.<br>Keeps access lists and user privileges information up to date. |

| Control | Description | Sophos solution | How it helps |
|---|---|---|---|
| | | 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.<br>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 Firewall | User awareness across all areas of our firewall governs all firewall polices and reporting, enabling user-level access controls.<br>Supports flexible multi-factor authentication options including directory services for access to key system areas. |
| | | 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 |
| | | 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. |
| **A 8.7: Protection Against Malware** | Protection against malware shall be implemented and supported by appropriate user awareness. | Sophos Intercept X<br>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.<br>Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers.<br>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.<br>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.<br>Sophos X-Ops experts keep operators up-to-date on the latest threat and vulnerability developments. |

| Control | Description | Sophos solution | How it helps |
|---|---|---|---|
| **A 8.8: Management of Technical Vulnerabilities** | Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken. | 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<br>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 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. |
| **A 8.9: Configuration Management** | Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed. | 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 | 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.<br>Administrators are instructed to change the default password of the "admin" user immediately after deployment. An alert is displayed when the default password for the super administrator is not changed. |
| **A 8.11: Data Masking** | Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration. | Sophos Firewall | Allows encryption of identities including user names, IP addresses, MAC addresses and email addresses in logs and reports.<br>Pre-defined administrative roles may be assigned to administrators restricting access to sensitive log data as well as restricting them from making changes to settings and configurations. |
| **A 8.12: Data Leakage Prevention** | Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information. | Sophos Firewall<br>Sophos Intercept X<br>Sophos Intercept X for Server | Data Leakage Prevention (DLP) capabilities in Sophos products can detect sensitive personal data 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.<br>Flexible compliance rules monitor device health and flag deviation from desired settings. |
| | | Sophos Managed Detection and Response (MDR) | 24/7 monitoring of the environment plus investigation and neutralization of malicious activities secures against data loss through adversarial activities. |
| | | Sophos ZTNA | Continuously validates user identity, device health, and compliance before granting access to applications and data. |
| | | Sophos Central Device Encryption | Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance. |

| Control | Description | Sophos solution | How it helps |
|---|---|---|---|
| | | Sophos Email | Prevent data loss by creating multi-rule DLP policies for groups and individual users to ensure the protection of sensitive information with discovery of confidential contents in all emails and attachments. |
| **A 8.13: Information Backup** | Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup. | 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. |
| **A 8.15: Logging** | Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed. | All Sophos products | Enables generation of 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. |
| | | 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. |
| **A 8.16: Monitoring Activities** | Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents. | Sophos Managed Detection and Response (MDR) | Our threat-hunting experts monitor and investigate alerts from across the network, leveraging network, firewall, cloud, email, and endpoint security tools to identify and investigate suspicious activities and protect personal data wherever it resides. Sophos NDR generates high-caliber actionable signals across the network infrastructure to optimize cyber defenses. |
| | | 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.<br>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. |
| **A 8.19: Installation of Software on Operational Systems** | Procedures and measures shall be implemented to securely manage software installation on operational systems. | Sophos Intercept X<br>Sophos Intercept X for Server | Blocks vulnerabilities in applications, operating systems, and devices with its exploit prevention capabilities. |
| **A 8.20: Networks Security** | Networks and network devices shall be secured, managed and controlled to protect information in systems and 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.<br>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) | 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 XDR | Detects and investigates across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action. |
| | | Synchronized Security in Sophos products | Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls. |
| | | 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. |

| Control | Description | Sophos solution | How it helps |
|---|---|---|---|
| **A 8.22: Segregation of Networks** | Groups of information services, users and information systems shall be segregated in the organization's networks. | 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.<br>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 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. |
| **A 8.23: Web Filtering** | Access to external websites shall be managed to reduce exposure to malicious content. | Sophos Intercept X<br>Sophos Intercept X for Server | Scans web content and allows category-based web filtering to be enforced both on and off the corporate network. |
| | | Sophos Intercept X for Mobile | Web filtering and URL checking stops access to known bad sites on mobile devices, while SMS phishing detection spots malicious URLs. |
| | | Sophos Firewall | Full visibility and control over all web traffic with flexible enforcement tools that work the way you need, with options for user and group enforcement of activity, quotas, schedules, and traffic shaping. Blocks known malicious domains and IP addresses through configuration of its web protection rule and FQDN host appropriately.<br>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. |
| **A 8.25: Secure Development Life Cycle** | Rules for the secure development of software and systems shall be established and applied. | Sophos Factory | Allows the introduction of static and dynamic security scanning and testing at any step of the app delivery process. Adds security to existing DevOps workflows by leveraging integrations with GitLab, GitHub, Bitbucket, and other git providers. |
| **A 8.26: Application Security Requirements** | Information security requirements shall be identified, specified and approved when developing or acquiring applications. | Sophos Intercept X<br>Sophos Intercept X for Server | Blocks vulnerabilities in applications, operating systems, and devices with its exploit prevention capabilities. |
| | | Sophos Factory | With Sophos Factory's automation pipelines, you can quickly introduce static and dynamic security scanning and testing at any step of the app delivery process. Add security to your existing DevOps workflows by leveraging integrations with GitLab, GitHub, Bitbucket, and other git providers. |
| **A 8.28: Secure Coding** | Secure coding principles shall be applied to software development. | Sophos Factory | Combines tools, teams, and practices to standardize, secure, and reuse IT as code pipelines. It enables you to build modern solutions through collaborative automation, empowering Dev, Sec, and Ops teams to build upon accumulated knowledge efficiently. |
| **A 8.29: Security Testing in Development and Acceptance** | Security testing processes shall be defined and implemented in the development life cycle. | Sophos Factory | With Sophos Factory's automation pipelines, you can quickly introduce static and dynamic security scanning and testing at any step of the app delivery process. Add security to your existing DevOps workflows by leveraging integrations with GitLab, GitHub, Bitbucket, and other git providers. |
| **A 8.31: Separation of Development, Test and Production Environments** | Development, testing and production environments shall be separated and secured. | Sophos Cloud Optix | Ensures container images and Infrastructure-as-Code (IaC) templates containing insecure configurations as well as embedded secrets and keys never make it to a test or live production environment. |

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

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

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

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



2023-04-05 CC (PC)

SOPHOS