HITRUST Common Security Framework

The HITRUST Common Security Framework (HITRUST CSF) is a certifiable framework that helps organizations blend their compliance requirements together with specific details on how controls are to be implemented. Built initially for organizations operating in the healthcare industry, the framework is industry-agnostic today. It aggregates requirements from multiple standards and frameworks like CMMS, ISO, PCI, and more, which allows organizations to take a comprehensive approach to secure their enterprise networks.

The HITRUST framework includes 156 controls and 75 control objectives. Each HITRUST control has three implementation levels: level one, level two, and level three. Level 1 is considered the baseline, while Level 3 has the greatest number of requirements and assures the greatest level of protection. Most organizations have varied levels of implementation based on their specific data protection needs and regulatory risk factors.

This document provides a general reference showing how some of Sophos products may assist organizations in implementing and managing their controls to meet compliance requirements.

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.

SOPHOS

Objective Name	Control Reference	Sophos Solution	How it helps
Control Category 01.0: Access Control			
01.01: Access Controls for Business Requirements	01.a: Create an access control policy	Sophos Firewall	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. 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 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 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.
01.02: Authorization for Access to Information Systems	01.c: Manage user privileges	Sophos Central	Configurable role-based administration provides granular control of administrator privileges. Keeps access lists and user privileges information up to date.
		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 Firewall	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling user-level access controls. 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.
	01.d: Manage user passwords	Sophos Firewall	Allows strong passphrase policy to be applied for admin accounts in terms of complexity, length, password reuse and use of a single dictionary word.
		Sophos Central	Disables or removes default passwords. Passwords are sufficiently complex to withstand targeted "brute force" attacks and must be rotated periodically.
	01.e: Monitor user access rights	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 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 Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.

Objective Name	Control Reference	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. 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 Central Device Encryption	Authenticates users for access to specific files/folders with the use of user- or group-specific keys.
		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.
01.04: Access Controls Regarding Network Traffic	01.i: Create a policy for network use	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	User awareness across all areas of our firewall governs all firewall policies and reporting, enabling user-level access controls over applications, websites, categories, and traffic shaping (QoS).
	01.j: Authenticate external connections	Sophos Wireless	Offers visibility into wireless network health and clients connecting to the network. Enhanced Rogue AP Detection classifies neighboring Wi-Fi networks to identify threats and prevent attempts to infiltrate an organization via Wi-Fi.
		Sophos Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. 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.
	01.l: Protect remote port configurations	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. Enables administrators to block or limit traffic to certain external systems with port-based or app-based policies.
		Sophos Cloud Optix	Cloud Optix continually monitors cloud resource configurations to identify issues such as exposed cloud server ports (e.g. RDP or SSH) that could be used in brute force cyberattacks.
	01.m: Segregate networks logically	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. 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.
		Sophos Wireless	Allows you to deploy a wireless guest network as a separate zone that allocates IP addresses from a defined range. You can block network access by specified hosts.

Objective Name	Control Reference	Sophos Solution	How it helps
	01.n: Controls network connections	Sophos Wireless	Enhanced Rogue AP Detection classifies neighboring Wi-Fi networks to identify threats and prevent attempts to infiltrate an organization via Wi-Fi. Enterprise-grade backend authentication provides controlled internet access and hotspots for visitors, contractors, and other guests on the network.
		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. Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
		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.
	01.o: Control routing to/ from networks	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.
		Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
		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.
01.05: Access Controls for Operating Systems	01.p: Control logon protocols	Sophos Firewall	Enables configuration to allow only a specific number of unsuccessful attempts before blocking suspicious login attempts.
	01.q: Control user authentication	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
		Sophos Central	Helps to protect 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 assess compliance.
	01.r: Manage password system(s)	Sophos Central	Disables or removes default passwords. Passwords are sufficiently complex to withstand targeted "brute force" attacks and must be rotated periodically.
		Sophos Firewall	Allows strong passphrase policy to be applied for admin accounts in terms of complexity, length, password reuse and use of a single dictionary word.
	01.t: Require session timeouts	Sophos Firewall	Automatically terminates a session or enforces session time-out after a specific time interval of user inactivity.
	01.u: Limit access session length	Sophos Firewall	Automatically terminates a session or enforces session time-out after a specific time interval of user inactivity.

Objective Name	Control Reference	Sophos Solution	How it helps
01.06: Access Controls for Application Information	01.v: Restrict access to sensitive data	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; enables detection of compromised / unauthorized endpoint device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.
		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. Enforces web, data, and device policies to allow only authorized applications to be run, devices to be connected and data to be distributed.
		Sophos Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
		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. And includes an IAM visualization tool that provides a complete map of IAM relationships and allows teams to quickly and easily identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks.
		Sophos Managed Detection and Response (MDR)	Sophos MDR continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events. Anomalous behaviors and code use are detected, investigated, and correlated to identify malicious activities and enable us to quickly neutralize the event
		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 Email	Allows 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	Enables protection of devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.

Objective Name	Control Reference	Sophos Solution	How it helps
01.07: Remote and Mobile Access Controls	01.x: Control for mobile computing	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 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 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.
	01.y: Designate controls for telework	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
		Sophos Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
		Sophos Mobile	Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. A rich set of device management capabilities, containers, and market-leading encryption helps to keep sensitive business email and documents protected on mobile devices – even for users working with personal devices. Leading antivirus and ransomware protection enables safeguarding your users and devices from malicious content and apps.
		Sophos Email	Allows 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.
Control Category 02.0: Human Resources			
02.04: HR Controls for Personnel Moves	02.i: Remove user access rights immediately	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 (e.g., because they change position or leave the company).

Objective Name	Control Reference	Sophos Solution	How it helps
Control Category 03.0: Risk Management			
03.01: Risk Management Program Controls	03.b: Regularly assess risk environment	Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
		Sophos XDR	Detect and investigate across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
		Sophos Firewall	Allows real-time insights into network and user events, quick and easy access to historical data, and easy integration with third-party remote management and monitoring tools (RMMs).
		Sophos 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 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.
	03.c: Execute risk mitigation strategies	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 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.

Objective Name	Control Reference	Sophos Solution	How it helps
		Sophos Cloud Optix	Cloud Optix allows security teams to focus on and fix their most critical public cloud security vulnerabilities before they are identified and exploited in cyberattacks. By identifying and risk-profiling security, compliance, and cloud spend risks, Cloud Optix enables teams to respond faster, providing contextual alerts that group affected resources with detailed remediation steps.
		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 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 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. Incidents are contained and neutralized with an 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 Wireless	Enhanced Rogue AP Detection classifies neighboring Wi-Fi networks to identify threats and prevent attempts to infiltrate an organization via Wi-Fi.
	03.d: Evaluate risks and root causes	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)	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.
		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	Provides 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).
		Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
		Sophos Intercept X Sophos Intercept X for Server	Get the root cause analysis of an attack with visibility on the how and where of the attack along with recommendations on what your next steps should be.

Objective Name	Control Reference	Sophos Solution	How it helps
Control Category 04.0: Security Policies			
04.01: Information Security Policy Controls	04.b: Review information security policies	Sophos Intercept X Sophos Intercept X for Server	Intercept X consistently looks at reported false positives and false negatives to ensure the product is being continuously improved. It integrates a deep learning malware detection model that can scale to hundreds of millions of training samples and can 'memorize' the entire observable threat landscape as part of its training process. It is regularly trained by our SophosLabs team to stay up to date over time.
		Sophos Managed Detection and Response (MDR)	Sophos MDR includes full incident response, delivered by a 24/7 team of response experts. Once an incident is remediated, Sophos MDR performs full root cause analysis which enables the environment to be hardened and response plans and strategies to be updated to incorporate learnings.
		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.
Control Category 05.0: Information Organization			
05.01: Controls for Internal Organization	05.c: Allocate information security responsibilities	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 Central	Does not permit shared administrator accounts. Each employee has his or her own account, with explicit permissions granted to each account. Enables protection of privileged and administrator accounts with advanced two-factor authentication.
05.02: Controls for External Organization	05.i: Identify risks related to all third parties	Sophos Intercept X Advanced with XDR	Provides comprehensive defense in depth against threats that get in via third party suppliers using AI, exploit prevention, behavioral protection, anti-ransomware and more. Plus, Sophos' XDR functionality enables automatic identification of suspicious activity, prioritizes threat indicators, and quickly searches for potential threats across endpoint and servers.
		Sophos Managed Detection and Response (MDR)	Delivers expert threat hunting and remediation as a fully-managed service. Sophos specialists work around the clock to proactively hunt for, validate, and remediate potential supply chain threats and incidents on your behalf.
	05.k: Implement vendor and partner security	Sophos Intercept X Advanced with XDR	Provides comprehensive defense in depth against threats that get in via third party suppliers using AI, exploit prevention, behavioral protection, anti-ransomware and more. Plus, Sophos' XDR functionality enables automatic identification of suspicious activity, prioritizes threat indicators, and quickly searches for potential threats across endpoint and servers.
		Sophos Managed Detection and Response (MDR)	Delivers expert threat hunting and remediation as a fully-managed service. Sophos specialists work around the clock to proactively hunt for, validate, and remediate potential supply chain threats and incidents on your behalf.
		Sophos ZTNA	Helps to safeguard against supply chain attacks that rely on supplier access to your systems via 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.
Control Category 06.0: Regulatory Compliance			
06.01: Legal Regulatory Compliance Controls	06.c: Protect critical internal records	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.

Objective Name	Control Reference	Sophos Solution	How it helps
		Sophos Central	Each employee has his or her own account, with explicit permissions granted to each account. Enables protection of privileged and administrator accounts with advanced two-factor authentication.
		Sophos Managed Detection and Response (MDR)	24/7 monitoring of the environment plus investigation and neutralization of malicious activities secures against data loss through adversarial activities.
		Sophos Firewall Sophos Intercept X 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 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.
		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.
	06.d: Protect "covered" data classes	Sophos Central Device Encryption	Enables protection of devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
		Sophos Intercept X Sophos Intercept X for Server	Endpoint Protection application control policies restrict the use of unauthorized applications. Device Control allows admins to control the use of removable media through policy settings. Anti-exploit, anti-ransomware, and deep learning malware detection enable protection of endpoints from malicious executable code.
		Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
		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 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 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 Mobile	Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. A rich set of device management capabilities, containers, and market-leading encryption helps to keep sensitive business email and documents protected on mobile devices – even for users working with personal devices. Leading antivirus and ransomware protection enables safeguarding your users and devices from malicious content and apps.

Objective Name	Control Reference	Sophos Solution	How it helps
	06.e: Prevent misuse of protected data	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – this helps to stop advanced attacks.
		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 Mobile	Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. A rich set of device management capabilities, containers, and market-leading encryption keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices.
		Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication.
		Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
		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.
	06.f: Implement cryptographic controls	Sophos Mobile	Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. A rich set of device management capabilities, containers, and market-leading encryption keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices.
		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 Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.
		Sophos Central Device Encryption	Enables protection of devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
06.02: Policy, Standard, and Technical Controls	06.g: Comply with security standards	Sophos Cloud Optix	Sophos Cloud automatically analyzes public cloud configuration settings against compliance and security best practice standards. The service continuously monitors compliance with custom or out-of-the box templates and audit-ready reports for standards such as FFIEC, GDPR, HIPAA, PCI DSS, and SOC2. Audit-ready reports then enable you to define which inventory items within your public cloud account are subject to certain compliance standards, reducing the hours associated with compliance audits.
	06.h: Check for technical compliance		

Objective Name	Control Reference	Sophos Solution	How it helps
06.03: Controls for Information System Audits	06.i: Audit controls for compliance	Sophos Cloud Optix	Sophos Cloud Optix reduces the cost and complexity of public cloud compliance with industry standards like SOC2, GDPR, PCI, and others. By automatically mapping security and compliance standards to your environments, Cloud Optix 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. Cloud Optix also helps teams to save weeks of effort by mapping the Control ID from existing overarching compliance tools such as RSA Archer or MetricStream to Cloud Optix.
	06.j: Store and protect audit logs	Sophos Firewall	Logs storage cannot access, destructed, or altered without administrator privileges. To prevent accidental destruction due to destruction of firewall device altogether, the logs can be integrated into independent syslog server or into Sophos Central.
Control Category 09.0: Communications and Operations			
09.04: Safeguards Against Malicious Code	09.j: Control malicious code	Sophos Cloud Optix	Enables continuous monitoring and detection of 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. 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	Enables detection of 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 Intercept X Sophos Intercept X for Server	Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers. Application Control policies restrict the use of unauthorized applications.
	09.k: Control mobile code	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 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.
09.05: Information Backup Controls	09.l: Perform routine data backups	Sophos Cloud Optix	Sophos 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.

Objective Name	Control Reference	Sophos Solution	How it helps
09.06: Controls Over Network Security	09.m: Monitor network traffic	Sophos Firewall	Provides real-time insights into network and user events, quick and easy access to historical data, easy integration with third-party remote management and monitoring tools (RMMs). Offers visibility into risky users, evasive and unwanted applications, and suspicious payloads. Synchronized Application Control automatically identifies unknown, evasive, and custom applications running on your network so you can easily prioritize the ones you want, and block the ones you don't.
		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.
		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)	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 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.
	09.n: Control network security	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 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 Managed Detection and Response (MDR)	Threat hunting experts monitor and correlate signals from across the network, identifying and investigating suspicious activities. Sophos NDR generates high caliber, actional signals across the network infrastructure to optimize cyber defenses.
		Sophos Rapid Response Service	Get fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
		Sophos 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.
09.07: Media Management Controls	09.o: Manage removable media	Sophos Intercept X Sophos Intercept X for Server	Device Control allows admins to control the use of removable media through policy settings.
	09.q: Control handling of data	Sophos Mobile	Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. Emails and documents can be stored in the secure and encrypted Sophos Container and accessed with the Sophos Secure Email and Sophos Secure Workspace apps.

Objective Name	Control Reference	Sophos Solution	How it helps
09.08: Controls for Information Exchange	09.v: Control electronic messaging, per policy	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.
	09.w: Control interconnected business systems	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.
09.10: Controls for Overall Monitoring	09.aa: Log all audit information	All Sophos products	Enables generation of security event logs that can be integrated into a centralized monitoring program for incident detection and response.
	09.ab: Monitor all use of systems	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.
		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 detects and investigates suspicious events from across the full security environment to identify threats and appropriate response activities. Data is collected across endpoint, network, identity email, and more, and then correlated using powerful AI tools, threat intelligence and human expertise to identify impact and response.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
		Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
	09.ad: Log all administrative audits	All Sophos products	All administrative actions are logged and available for reporting and audits.

Objective Name	Control Reference	Sophos Solution	How it helps
		Control Category 10.0: Data Systems Management	
10.06: Vulnerability Management Controls	10.m: Manage security vulnerabilities	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	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 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)	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 fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
		Sophos Intercept X Sophos Intercept X for Server	HIPS, deep learning, anti-exploit, anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host. Endpoint Protection application control policies restrict the use of unauthorized applications.
		Control Category 11.0: Incident Management	
11.01: Incident and Weakness Reporting Protocols	11.a: Report on cybersecurity events	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
		Sophos Rapid Response Service	Get fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
		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.
	11.b: Report cybersecurity weaknesses	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	Get fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
		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 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.

Objective Name	Control Reference	Sophos Solution	How it helps
11.02: Incident and Improvement Management Controls	11.d: Mobilize data from past security events	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)	Full incident response service included as standard, providing 24/7 coverage delivered by IR experts. Includes full root cause analysis and reporting.
	11.e: Collect evidence from all security events	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.
Control Category 12.0: Business Continuity			
12.01: Continuity and Information Security Controls	12.c: Integrate security and continuity implementation	Sophos Email	In the event of third-party cloud email service provider outages, alerts are provided if mail can't be delivered to a server/service; email is then queued for delivery to help protect against lost email, and access to that queued email is provided from a 24/7 emergency inbox inside the end user portal. Retry period for queued email is 5 days.
		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

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

2022-12-01 CC (MP)

SOPHOS