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, that allows organizations to take a comprehensive approach to secure their enterprise networks.

Currently in its version 9, 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.

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	Allows user awareness across all areas of our firewall governs all firewall polices and reporting, enabling user-level control over applications, bandwidth and other network resources.
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. Protects privileged and administrator accounts with advanced two-factor authentication. 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).
	01.d: Manage user passwords	Sophos Firewall	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.
	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.

SOPHOS

Objective Name	Control Reference	Sophos Solution	How it helps*
		Sophos Cloud Optix	Enables adoption of the principle of least privilege across public cloud environments with Sophos Cloud Optix, Cloud Security Posture Management solution. The SaaS based service connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real time to identify possible credential misuse or theft. Includes an IAM visualization tool that provides a complete map of IAM relationships and allows teams to quickly and easily identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks.
		Sophos Zero Trust Network Access	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	Encrypts documents within a secure container on a mobile device managed with Sophos Mobile. Sophos Secure Workspace can dynamically encrypt content sent to cloud-based storage services and applications. It enables enforcement of device encryption and monitors compliance relative to encryption policy.
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.
	01.j: Authenticate external connections	Sophos Wireless	Offers visibility into wireless networks health and clients connecting to the network. With visibility into potential threats, such as rogue APs, insight into clients with compliance or connectivity issues and advanced diagnostics, identifying and troubleshooting issues is quick and easy. 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 Zero Trust Network Access	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. Lateral Movement Protection, a Synchronized Security feature, is designed to help prevent the threat or hacker from spreading to other systems, stealing data, or communicating back to the host.
		Sophos Wireless	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. 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	Offers visibility into wireless networks health and clients connecting to the network. With visibility into potential threats, such as rogue APs, insight into clients with compliance or connectivity issues and advanced diagnostics, identifying and troubleshooting issues is quick and easy. 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.
		Sophos Cloud Optix	Analyzing public cloud network security group configurations, Cloud Optix can visualize network traffic patterns to identify both actual and potential traffic routes that could be exploited. Cloud Optix utilizes Sophos AI to analyze network traffic and identify unusual patterns that could indicate a breach in security.
	01.o: Control routing to/ from networks	Sophos Firewall	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. Lateral Movement Protection, a Synchronized Security feature, is designed to help prevent the threat or hacker from spreading to other systems, stealing data, or communicating back to the host.
		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 Zero Trust Network Access	Validates user identity, device health, and compliance before granting access to resources.
		Sophos Firewall	Sophos Firewall with Security Heartbeat™ allows next-generation endpoint and network security to continuously share meaningful information about suspicious events across extended IT ecosystem; helps detect compromised / unauthorized endpoint device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.
		Sophos Central	Helps to protect privileged and administrator accounts with advanced two-factor authentication.
		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 enables protection of sensitive business email and documents on mobile devices – even for users working with personal devices. Leading antivirus and ransomware protection helps to safeguard your users and devices from malicious content and apps.
		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. Authenticates users for access to specific protected devices, files, and/or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication.
		Sophos 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.

Objective Name	Control Reference	Sophos Solution	How it helps*
	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.
01.06: Access Controls for Application Information	01.v: Restrict access to sensitive data	Sophos Zero Trust Network Access	Validates user identity, device health, and compliance before granting access to resources.
		Sophos Firewall	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 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 allows 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.
		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. Authenticates users for access to specific protected devices, files, and/or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication.
01.07: Remote and Mobile Access Controls	01.x: Control for mobile computing	Sophos Wireless	Offers visibility into wireless networks health and clients connecting to the network. With visibility into potential threats, such as rogue APs, insight into clients with compliance or connectivity issues and advanced diagnostics, identifying and troubleshooting issues is quick and easy. Enhanced Rogue AP Detection classifies neighboring Wi-Fi networks and allows to identify threats and prevent attempts to infiltrate an organization via Wi-Fi.
		Sophos Mobile	Provides enterprise mobility and security management capabilities for traditional and mobile endpoints, including security and device policies. Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. Emails and documents can be stored in the secure and encrypted Sophos Container and accessed with the Sophos Secure Email and Sophos Secure Workspace apps. The Sophos Secure Workspace app enables security of sensitive data with AES-256 encryption, allowing a secure way to manage, distribute, and edit documents and view web content on mobile devices. Web filtering and URL checking stops access to known bad sites on mobile devices, while SMS phishing detection spots malicious URLs.
	01.y: Designate controls for telework	Sophos Zero Trust Network Access	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.

Objective Name	Control Reference	Sophos Solution	How it helps*
		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.
		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. Authenticates users for access to specific protected devices, files, and/or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication.
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).
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 Intercept X Advanced with 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 Firewall	Allows real-time insights into network and user events, quick and easy access to historical data, and easy integration with third-party remote management and monitoring tools (RMMs).
		Sophos Managed Threat Response (MTR)	Helps to proactively hunt threats 24x7 and neutralize even the most sophisticated threats with Sophos' managed detection and response services backed by an elite team of threat hunters and response experts who take targeted actions on your behalf
		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	Enables role-based administration for delegating secure network security management; blocks traffic, services, ports and protocols except those explicitly allowed and defined as appropriate and necessary for the organization. Includes IPS, APT, AV, sandboxing with deep learning, and web protection to monitor and block malicious, anomalous, and exploitive traffic from inbound or outbound access. Sophos Sandstorm, optional cloud-sandbox technology, inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.
		Sophos Intercept X Sophos Intercept X for Server	HIPS, Deep Learning, Anti-exploit, Anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host.

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.
		Sophos Managed Threat Response (MTR)	Proactive 24/7 threat hunting by elite team of threat analysts initiates actions to remotely disrupt, contain, and neutralize threats on your behalf to stop sophisticated threats. Investigates detections from Sophos-protected endpoints, networks, and cloud platforms on customers' behalf to validate if adversarial activity or an active threat exists. Depending on the customer preference, notification of findings and recommendations are shared or an immediate response to the threat is initiated. Performs thorough investigations of detections, telemetry, and other datasets (observables) to derive indicators for use in threat hunts and targeted response actions. Incorporates vulnerability intelligence to provide customers with proactive security posture improvements.
		Security Consulting	Sophos offers penetration testing and vulnerability assessment of security infrastructure and software deployments; and recommendations for architecture and design changes needed to better use the available infrastructure.
		Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
		Sophos Email Sophos Firewall	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine helps to catch the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam. Sophos SPX encryption provides encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to enable compliance.
		Sophos Wireless	Offers visibility into wireless networks health and clients connecting to the network. With visibility into potential threats, such as rogue APs, insight into clients with compliance or connectivity issues and advanced diagnostics, identifying and troubleshooting issues is quick and easy. Enhanced Rogue AP Detection classifies neighboring Wi-Fi networks to identify threats and prevent attempts to infiltrate an organization via Wi-Fi.
		Sophos Mobile	Provides enterprise mobility and security management capabilities for traditional and mobile endpoints, including security and device policies. Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. Emails and documents can be stored in the secure and encrypted Sophos Container and accessed with the Sophos Secure Email and Sophos Secure Workspace apps. The Sophos Secure Workspace app enables security of sensitive data with AES-256 encryption, allowing a secure way to manage, distribute, and edit documents and view web content on mobile devices.
	03.d: Evaluate risks and root causes	Sophos Intercept X Advanced with XDR	Enable detection and investigation across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
		Sophos Managed Threat Response (MTR)	Monitors and investigates detections from Sophos endpoint, network, and cloud platform solutions to help you identify, investigate, contain, and neutralize active threats.
		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).
		Sophos Central Management	Provides centralized management and reporting for all Sophos products from a single console.

Objective Name	Control Reference	Sophos Solution	How it helps*
		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.
Control Category 04.0: Security Policies			
04.01: Information Security Policy Controls	04.a: Document information security practices	Sophos Cloud Optix	Sophos Cloud Optix, enables teams to proactively improve public cloud security posture, detecting insecure configurations and vulnerabilities. By automatically mapping regulatory compliance, security best practice standards, and your own custom security policies to cloud environments Cloud Optix provides the visibility needed to monitor and maintain security posture 24/7.
	04.b: Review information security policies		
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.
		Sophos Cloud Optix	Cloud Optix allows teams to embed cloud security and compliance response into standard workflows by creating Jira and ServiceNow tickets from inside the Cloud Optix console for new Sophos Cloud Optix alerts. Two-way integration avoids duplication by enabling existing tickets for the same issue type to be updated if present before a new ticket is created.
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 Threat Response (MTR)	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 Threat Response (MTR)	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 Zero Trust Network Access	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 Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
		Sophos Cloud Optix	Cloud Optix continually monitors public cloud infrastructure to provide visibility of resources and threats across your organization and proactively reduce business risk from unsanctioned activity, vulnerabilities, and misconfigurations that would leave internal records exposed.
		Sophos Zero Trust Network Access	Continuously validates user identity, device health, and compliance before granting access to applications and data.
		Sophos Central Device Encryption	Enables user authentication for access to specific files/folders with the use of user- or group-specific keys.
		Sophos Mobile	Encrypts documents within a secure container on a mobile device managed with Sophos Mobile. Sophos Secure Workspace can dynamically encrypt content sent to cloud-based storage services and applications. It allows enforcement of device encryption and monitors compliance relative to encryption policy.
	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. Enables user authentication for access to specific protected devices, files, and/or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication.
		Sophos 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 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.
	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 Intercept X Advanced with 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 Zero Trust Network Access	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. 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.

Objective Name	Control Reference	Sophos Solution	How it helps*
		Sophos Managed Threat Response (MTR)	Proactive 24/7 threat hunting by elite team of threat analysts initiates actions to remotely disrupt, contain, and neutralize threats on your behalf to stop sophisticated threats. Investigates detections from Sophos-protected endpoints, networks, and cloud platforms on customers' behalf to validate if adversarial activity or an active threat exists. Depending on the customer preference, notification of findings and recommendations are shared or an immediate response to the threat is initiated.
	06.f: Implement cryptographic controls	Sophos Mobile	Encrypts documents within a secure container on a mobile device managed with Sophos Mobile. Sophos Secure Workspace can dynamically encrypt content sent to cloud-based storage services and applications. It enables enforcement of device encryption and monitors compliance relative to encryption policy.
		Sophos Central Device Encryption	Enables protection of devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance. Authenticates users for access to specific protected devices, files, and/or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication.
		Sophos Email	Offers TLS encryption and support for SMTP/S along with full push-base, and optional pull-based portal encryption.
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		
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		
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 Server	Facilitates prevention of unauthorized applications from running , automatically scanning your system for known good applications, and whitelisting only those applications.
		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.

Objective Name	Control Reference	Sophos Solution	How it helps*
		Sophos Managed Threat Response (MTR)	Incorporates vulnerability intelligence to provide customers with proactive security posture improvements.
		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 Intercept X for Mobile	Facilitates 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 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	Browser exploit prevention detects and blocks malicious activity attempting to take advantage of software vulnerabilities. Web security and web control scans the web content and can limit access to known sites.
		Sophos Firewall	Does not permit known malicious domains and IP addresses through configuration of its web protection rule and FQDN host appropriately. 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.
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.
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 Intercept X Advanced with 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 Threat Response (MTR)	Proactively hunt threats 24x7 and neutralize sophisticated threats with our managed detection and response services backed by an elite team of threat hunters and response experts who take targeted actions on your behalf.
		Sophos Cloud Optix	Analyzing public cloud network security group configurations, Cloud Optix can visualize network traffic patterns to identify both actual and potential traffic routes that could be exploited. Cloud Optix utilizes Sophos AI to analyze network traffic and identify unusual patterns that could indicate a breach in security.
	09.n: Control network security	Sophos Zero Trust Network Access	Continuously validates user identity, device health, and compliance before granting access to applications and data.
		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.

Objective Name	Control Reference	Sophos Solution	How it helps*
		Sophos Firewall	Includes next-gen IPS that offers advanced protection from hacks and attacks using a uniform signature format backed by SophosLabs. Besides traditional servers and network resources, it also helps to identify and protect users and applications on the network. 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 Lateral Movement Protection, a Synchronized Security feature, is designed to prevent the threat or hacker from spreading to other systems, stealing data, or communicating back to the host.
		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 Threat Response (MTR)	Proactively hunt threats 24x7 and neutralize sophisticated threats with our managed detection and response services backed by an elite team of threat hunters and response experts who take targeted actions on your behalf.
		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 Advanced with 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.
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.
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 ACE	Brings together the power of Sophos' threat intelligence, next-gen technologies, data lake, APIs, and Sophos Central management platform, creating an adaptive cybersecurity ecosystem that constantly learns and improves. This addresses the new reality of human-led hacking while supporting today's interconnected, digital world.
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.

Objective Name	Control Reference	Sophos Solution	How it helps*
		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.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.
		Sophos Intercept X Advanced with XDR	Enables detection, investigation, and response to suspicious endpoint activity.
		Sophos Firewall	Facilitates remote access authentication and user monitoring for remote access, and logs all access attempts.
		Sophos Mobile	Creates detailed log events of all malicious activity on mobile devices, helping to identify suspicious activity that may try to access sensitive data.
	09.ad: Log all administrative audits	All Sophos products	All administrative actions are logged and available for reporting and audits.
		Sophos Central	Configurable role-based administration provides granular control of administrator privileges.
		Sophos Firewall Manager	Offers role-based administration with change control and logging.
Control Category 10.0: Data Systems Management			
10.06: Vulnerability Management Controls	10.m: Manage security vulnerabilities	Sophos Firewall	Includes next-gen IPS that offers advanced protection from hacks and attacks using a uniform signature format backed by SophosLabs. Besides traditional servers and network resources, it also enables identification and protection of users and applications on the network. 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 Lateral Movement Protection, a Synchronized Security feature, is designed to prevent the threat or hacker from spreading to other systems, stealing data, or communicating back to the host.
		Sophos Cloud Optix	Sophos's cloud security posture management solution, Sophos Cloud Optix, enables teams to proactively improve security posture, detecting insecure configurations and vulnerabilities. By automatically mapping security and compliance standards to your environments, Cloud Optix provides the visibility needed to monitor and maintain security posture 24/7.
		Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
		Sophos Managed Threat Response (MTR)	Proactively hunt threats 24x7 and neutralize sophisticated threats with our managed detection and response services backed by an elite team of threat hunters and response experts who take targeted actions on your behalf.
		Sophos Rapid Response Service	Get fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.

Objective Name	Control Reference	Sophos Solution	How it helps*
		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. Exploit prevention capabilities do not permit vulnerabilities in applications and operating systems from being exploited by attackers. Endpoint Protection application control policies restrict the use of unauthorized applications. Server Lockdown allows only trusted whitelisted applications and associated files to run.
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 Threat Response (MTR)	Proactively hunt threats 24x7 and neutralize sophisticated threats with our managed detection and response services backed by an elite team of threat hunters and response experts who take targeted actions on your behalf.
		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 Threat Response	Proactively hunt threats 24x7 and neutralize sophisticated threats with our managed detection and response services backed by an elite team of threat hunters and response experts who take targeted actions on your behalf.
		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.
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.
	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.

Objective Name	Control Reference	Sophos Solution	How it helps*
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.

*Specifications and descriptions are subject to change without notice, and products may require configuration and/or enablement as applicable to achieve desired functionality. 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.

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

2021-10-19 CC (PC)

SOPHOS