NIST SP800-171

NIST SP800-171 is a codification of the requirements that any non-federal computer system must follow in order to store, process, or transmit Controlled Unclassified Information (CUI) or provide security protection for such systems. This set of guidelines imposes administrative and technical requirements on contractors and sub-contractors of federal agencies to ensure that sensitive federal information remains confidential when stored in non-federal information systems and organizations. First published in 2015 by the National Institute of Standards and Technology (NIST), NIST SP800-171 went into full effect in 2017 and has been updated several times since then.

This document maps out how Sophos solutions offer effective tools to help address some of the requirements as part of a customer's efforts to comply with NIST SP800-171.

Specifications and descriptions are subject to change without notice. Sophos disclaims all warranties and guarantees regarding this information. The 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.

No.	Security Requirements	Sophos Solution	How It Helps
3.1 Access Control			
Basic Security Requirements			
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Sophos Firewall	User awareness across all areas of our firewall governs all firewall policies and reporting, giving user-level controls over applications, bandwidth, and other network resources. Supports flexible multi-factor authentication options, including directory services, for access to key system areas.
		Sophos Central Device Encryption	Enables protection of devices and data with full disk encryption for Windows and macOS.
		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 can automatically deny access to sensitive data in case of a compromised device.
		Sophos Cloud Optix	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.

No.	Security Requirements	Sophos Solution	How It Helps
		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).
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	Sophos Firewall	User awareness across all areas of our firewall governs all firewall policies and reporting, giving user-level controls over applications, bandwidth, and other network resources. Supports flexible multi-factor authentication options including directory services for access to key system areas.
		Sophos Central Device Encryption	Enables protection of devices and data with full disk encryption for Windows and macOS.
		Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms.
		Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
		Sophos Managed Detection and Response (MDR)	Sophos MDR continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events. Anomalous behaviors and code use are detected, investigated, and correlated to identify malicious activities and enable us to quickly neutralize the event.
		Sophos Network Detection and Response (NDR)	Continuously analyzes traffic for suspicious patterns. It works with your managed endpoints and firewalls to monitor network activity for suspicious and malicious patterns that your endpoints and firewalls cannot see. It detects abnormal traffic flows from unmanaged systems and IoT devices, rogue assets,insider threats, previously unseen zero-day attacks, and unusual patterns deep within the network.
		Sophos Cloud Optix	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	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.

No.	Security Requirements	Sophos Solution	How It Helps
Derived Security Requirements			
3.1.3	Control the flow of CUI in accordance with approved authorizations.	Sophos Firewall	User awareness across all areas of Sophos firewall governs all firewall policies and reporting, enabling user-level control over applications, bandwidth and other network resources. 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 Cloud Optix	Connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real time to identify credential misuse or theft. It includes an IAM visualization tool that provides a complete map of IAM relationships and allows teams to quickly and easily identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks.
		Sophos Switch	Allows network access control that enables you to authenticate users using LDAP, MAC address, or other authentication methods to connect to a network. This prevents unauthenticated users and devices from gaining access to your LAN.
		Sophos 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.
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	All Sophos products	Sophos' user-identity-based policy technology allows user-level controls over network resources and other organization 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.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Sophos Cloud Optix	Connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real time to identify credential misuse or theft. It includes an IAM visualization tool that provides a complete map of IAM relationships and allows teams to quickly and easily identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks.
		Sophos Central	Configurable role-based administration provides granular control of administrator privileges. It keeps access lists and user privileges information up to date and protects privileged and administrator accounts with advanced two-factor authentication. Does not permit shared administrator accounts. Each employee has his or her own account, with explicit permissions granted to each account.
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		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 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.

No.	Security Requirements	Sophos Solution	How It Helps
3.1.12	Monitor and control remote access sessions.	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos Firewall	Controls remote access authentication and user monitoring for remote access and logs all access attempts.
		Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data. It authenticates requests for access from trusted users, irrespective of the location.
		Sophos Wireless	Monitors the health status of any Sophos-managed endpoint or mobile device and automatically restricts web access on trusted Wi-Fi networks for those with serious compliance issues.
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Sophos Email	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 ensure compliance.
		Sophos Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. The Sophos Cryptographic Module incorporated into the Sophos Firewall systems provides FIPS 140-2 validated cryptography for the protection of sensitive information.
		Sophos Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos-managed networks and hotspots.
3.1.14	Route remote access via managed access control points.	Sophos Wireless	Automatically controls access for Sophos-managed clients based upon their health status. Web access is restricted on trusted Wi-Fi networks for non-compliant devices.
3.1.16	Authorize wireless access prior to allowing such connections.	Sophos Wireless	Monitors the health status of any Sophos-managed endpoint or mobile device and automatically restricts web access on trusted Wi-Fi networks for those with serious compliance issues. Provides controlled internet access and hotspots for visitors, contractors, and other guests on the network using enterprise-grade backend authentication for a seamless user experience.
3.1.17	Protect wireless access using authentication and encryption.	Sophos Wireless	Enterprise-grade backend authentication provides seamless and controlled internet access and hotspots for visitors, contractors, and other guests on the network. Dynamic encrypted Wi-Fi sessions protect the information in transit on Sophos-managed networks and hotspots.
3.1.18	Control connection of mobile devices.	Sophos Intercept X for Mobile	Integration with Microsoft Intune allows administrators to build conditional access policies, restricting access to applications and data when a threat is detected.
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.	Sophos Mobile	Ensures the integrity of sensitive data on the mobile devices that your employees use to access your company database and other corporate resources. It promotes device encryption and ensures you can deny access to emails, networks, and other resources if a device does not comply with your company's policies.
3.2 Awareness and Training			
Basic Security Requirements			
3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	Sophos Training and Certifications	Training courses and certifications to help partners and customers get the best out of Sophos security deployments and access to the latest know-how and expertise for security best practices.
		Sophos Phish Threat	Provides simulated phishing cyberattacks and security awareness training for the organization's end users. Courses cover a wide range of topics, from phishing and cybersecurity overview lessons to data loss prevention, password protection, and more.

No.	Security Requirements	Sophos Solution	How It Helps
Derived Security Requirements			
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Sophos Phish Threat	Provides simulated phishing cyberattacks and security awareness training for the organization's end users. Courses cover a wide range of topics, from phishing and cybersecurity overview lessons to data loss prevention, password protection, and more. Sophos Phish Threat connects with Sophos Email to identify those who have a high risk profile. You can then seamlessly enroll them into targeted phishing simulations and training to improve awareness and cut your risk of attack.
3.3 Audit and Accountability			
Basic Security Requirements			
3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos Intercept X Sophos Intercept X for Server	Creates detailed log events for all malicious activity on endpoint systems, helping to identify suspicious activity on systems that may store or process CUI.
		Sophos Firewall	Allows real-time insights into network and user events and quick and easy access to historical data. It retains finite logs on the device itself and also summarizes the logs in the form of drill-down on-appliance reports for analysis. The logs can also be integrated into an independent external Syslog server or Sophos Central for analysis.
		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 endpoints, networks, identity, email, and more, and then correlated using powerful AI tools, threat intelligence, and human expertise to identify impact and response.
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	All Sophos products	Sophos' user-identity-based technology powers all policies and reporting across all Sophos products. This allows organizations to enforce role-based user-level controls over network resources and other organizational assets and trace the actions of individual users.
		Synchronized Security feature in Sophos product	The Synchronized User ID feature shares user identity between Sophos Endpoint Protection and Sophos Firewall, making user identity completely transparent and trouble-free.
Derived Security Requirements			
3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Sophos Firewall	Stored logs cannot be accessed, destroyed, or altered without administrator privileges. To prevent accidental destruction due to the destruction of the firewall device altogether, the logs can be integrated into an independent Syslog server or Sophos Central.

No.	Security Requirements	Sophos Solution	How It Helps
3.4 Configuration Management			
Basic Security Requirements			
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles	Sophos Cloud Optix	Offers inventory management across multiple cloud providers with continuous asset monitoring and complete network topology and traffic visualization. It establishes guardrails to prevent, detect, and remediate accidental or malicious changes in network configuration, network traffic, resource configuration, and user behavior or activities.
Derived Security Requirements			
3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.	All Sophos products	All administrative actions are logged and available for reporting and audits.
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	Sophos Firewall	User awareness across all areas of our firewall governs all firewall policies and reporting, enabling user-level access controls. Supports flexible multi-factor authentication options including directory services for access to key system areas.
3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	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.
3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	Sophos Firewall	Synchronized Application Control in Sophos Firewall identifies all networked applications in the environment running on Sophos-managed endpoints. User-based application policies enable custom-tailored application control to be added to any user, group, or network policy with the option also to apply traffic shaping.
		Sophos Intercept X Sophos Intercept X for Server	Endpoint Protection application control policies restrict the use of unauthorized applications.
		Sophos Intercept X for Server	Integrates server application whitelisting/lockdown with advanced anti-malware and HIPS that allows application whitelisting at the click of a button and permits only trusted applications.
3.4.9	Control and monitor user-installed software.	Sophos Mobile	Monitor devices for jailbreaking and application sideloading and deny access to email, network, and other resources if the device is not in compliance with the policy.
		Sophos Intercept X Sophos Intercept X for Server	Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers. Endpoint Protection application control policies restrict the use of unauthorized applications.
		Sophos 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 Firewall	Provides 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). It ensures 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.

No.	Security Requirements	Sophos Solution	How It Helps
3.5 Identification and Authentication			
Basic Security Requirements			
3.5.1	Identify system users, processes acting on behalf of users, and devices.	Sophos Firewall	User awareness across all areas of our firewall governs all firewall policies and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group.
		All Sophos products	Sophos' user-identity-based technology powers all policies and reporting across all Sophos products. This allows organizations to enforce role-based user-level controls over network resources and other organizational assets and trace the actions of individual users.
		Sophos Cloud Optix	Connects disparate actions with Sophos AI to identify unusual user access patterns and locations to identify credential misuse or theft. Ensures all identities only perform actions that are required for their tasks and nothing more.
3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	Sophos Firewall	Supports flexible multi-factor authentication options including directory services for access to key system areas.
		Sophos Switch	Allows network access control that enables user authentication using LDAP, MAC address, or other authentication methods to connect to a network. This prevents unauthenticated users and devices from gaining access to the LAN.
		Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
		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. Denies access to email, network, and other resources if the device is not in compliance with the policy.

No.	Security Requirements	Sophos Solution	How It Helps
Derived Security Requirements			
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	Sophos Firewall	Supports flexible multi-factor authentication options including directory services for access to key system areas.
		Sophos Switch	Allows network access control that enables user authentication using LDAP, MAC address, or other authentication methods to connect to a network. This prevents unauthenticated users and devices from gaining access to the LAN.
		Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication. Keeps access lists and user privileges information up to date. Provides procedures 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).
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	Sophos Central	Disables or removes default passwords. Passwords are sufficiently complex to withstand targeted "brute force" attacks and must be rotated periodically.
		Sophos Firewall	Ensures strong passphrase policy to be applied for admin accounts in terms of complexity, length, password reuse and use of a single dictionary word.
3.5.8	Prohibit password reuse for a specified number of generations.	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.
3.6 Incident Response			
Basic Security Requirements			
3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	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.
		All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms. Includes rollback to original files after a ransomware or master boot record attack. Provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware.
		Sophos Managed Detection and Response (MDR)	Sophos MDR detects and investigates suspicious events from across the full security environment to identify threats and appropriate response activities. Data is collected across endpoint, network, identity email, and more, and then correlated using powerful AI tools, threat intelligence and human expertise to identify impact and response.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
		Sophos Cloud Optix	Scans cloud resources for security misconfigurations, profiling any alerts by risk level to help teams focus on the priority areas, and provide detailed remediation guidance to fix those issues.
		Sophos Firewall	Uniquely integrates with Sophos Endpoint, Sophos XDR, and Sophos MDR to automatically respond to any threat or attack identified at the firewall, the endpoint, or by a security analyst. It automatically isolates compromised hosts, preventing lateral movement and external communications until a threat can be investigated and cleaned up.
		Sophos Network Detection and Response (NDR)	When Sophos NDR identifies an indicator of compromise, active threat, or adversary, analysts are immediately alerted and can instantly push a threat feed to Sophos Firewall to trigger an automated response to isolate the compromised host.

No.	Security Requirements	Sophos Solution	How It Helps
3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	Sophos Managed Detection and Response (MDR)	Sophos MDR includes full incident response, delivered by a dedicated team of response specialists who are experts at battling adversaries. Clear procedures and documentation enable consistent information sharing.
3.8 Media Protection			
Derived Security Requirements			
3.8.7	Control the use of removable media on system components.	Sophos Intercept X Sophos Intercept X for Server	Device Control allows admins to control the use of removable media through policy settings.
3.9 Personnel Security			
Basic Security Requirements			
3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	Sophos Firewall	Supports flexible multi-factor authentication options including directory services for access to key system areas.
		Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication.
		Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
		Sophos Mobile	Ensures the integrity of sensitive data on the mobile devices that your employees use to access your company database and other corporate resources. It promotes device encryption and ensures you can deny access to emails, networks, and other resources if a device does not comply with your company's policies.
3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Sophos Central	Keeps access lists and user privileges information up to date. Provides procedures 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).

No.	Security Requirements	Sophos Solution	How It Helps
3.11 Risk Assessment			
Basic Security Requirements			
3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
		Sophos XDR	Detects and investigates across endpoints, servers, firewalls, and other data sources. Provides a holistic view of 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 Network Detection and Response (NDR)	Continuously analyzes traffic for suspicious patterns. It works with Sophos-managed endpoints and firewalls to monitor network activity for suspicious and malicious patterns. It detects abnormal traffic flows from unmanaged systems and IoT devices, rogue assets, insider threats, previously unseen zero-day attacks, and unusual patterns deep within the network.
		Sophos Cloud Optix	Cloud Optix enables organizations to design public cloud environments to meet Amazon Web Services, Microsoft Azure, and Google Cloud Platform security best practice standards and maintain them. This agentless service continually monitors public cloud resources, providing the visibility to proactively identify unsanctioned activity, vulnerabilities, and misconfigurations.
		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	Provides incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
		All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
Derived Security Requirements			
3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Sophos Firewall	Provides 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). Allows fully automated application security with pre-defined policy templates for commonly used enterprise applications / software packages.
		Sophos Mobile	Monitors mobile devices for jailbreaking and application sideloading. Denies access to email, network, and other resources if device is not in compliance with policy.
		Synchronized Security in Sophos products	Sophos Firewall's Synchronized Security Endpoint Integration identifies all unknown, evasive, and custom applications running on your network so you can easily identify rogue applications like Psiphon and block them.
		Sophos Cloud Optix	Scans cloud resources for security misconfigurations, profiling any alerts by risk level to help teams focus on the priority areas, and provide detailed remediation guidance to fix those issues.
		Sophos Managed Detection and Response (MDR)	Sophos MDR investigates and assesses potential security risks across the full environment 24/7, leveraging world-leading threat intelligence from Sophos X-Ops to identify risk level and prioritize response.

No.	Security Requirements	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. Endpoint Protection application control policies restrict the use of unauthorized applications. Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers.
3.11.3	Remediate vulnerabilities in accordance with risk assessments.	Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
		Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
		Sophos Firewall	Uniquely integrates with Sophos Endpoint, Sophos XDR, and Sophos MDR to automatically respond to any threat or attack identified at the firewall, the endpoint, or by a security analyst. It automatically isolates compromised hosts, preventing lateral movement and external communications until a threat can be investigated and cleaned up.
		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	Enables 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	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.
3.12 Security Assessment			
Basic Security Requirements			
3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms.
		Sophos Managed Detection and Response (MDR)	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 Firewall	Includes the latest advanced protection technologies and threat intelligence, such as TLS 1.3 and DPI inspection, machine learning, and cloud sandboxing. It uniquely integrates with Sophos Endpoint, Sophos XDR, and Sophos MDR to automatically respond to any threat or attack identified at the firewall, the endpoint, or by a security analyst, automatically isolating compromised hosts, preventing lateral movement and external communications until a threat can be investigated and cleaned up.
		Sophos Cloud Optix	Proactively identifies unsanctioned activity, vulnerabilities, and misconfigurations across AWS, Azure, and GCP. Complete cloud edge firewall solution includes IPS, ATP, and URL filtering and lets you deploy several network security products at once to protect your hybrid cloud environments against network threats.
		Sophos Network Detection and Response (NDR)	Continuously analyzes traffic for suspicious patterns, working with Sophos-managed endpoints and firewalls to monitor network activity for suspicious and malicious patterns. It detects abnormal traffic flows from unmanaged systems and IoT devices, rogue assets, insider threats, previously unseen zero-day attacks, and unusual patterns deep within the network.

No.	Security Requirements	Sophos Solution	How It Helps
3.13 System and Communications Protection			
Derived Security Requirements			
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	Sophos Firewall Sophos Intercept X Sophos Intercept X for Server	Data Leakage Prevention (DLP) capabilities in Sophos products can detect sensitive data and prevent leaks of such information via email, uploads, and local copying.
		Sophos Intercept X Sophos Intercept X for Server	Device Control allows admins to control the use of removable media through policy settings.
		Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS.
		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.
3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Sophos Firewall	Flexible and powerful segmentation options via zones and VLANs provide ways to separate levels of trust on your network while enabling added protection against lateral movement between different parts of your network.
		Sophos Switch	Allows configuration of VLANs to segment your internal traffic and reduce the attack surface in case of an infection or breach. Allows network access control that enables you to authenticate users using LDAP, MAC address, or other authentication methods to connect to a network. This prevents unauthenticated users and devices from gaining access to your LAN.
		Sophos Mobile	Supports BYOD environments through the Android Enterprise Work Profile and iOS User Enrolment modes of management. Corporate emails and apps can be deployed to a device while these remain separate from a user's personal data. Admins retain control over corporate content without intruding on the users' privacy.
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Sophos Email	Automatically scans message bodies and attachments for sensitive data, allowing you to easily establish policies to block or encrypt messages with just a few clicks. Sophos Email Offers TLS encryption and support for SMTP/S along with push-based encryption to send encrypted emails and attachments as password protected documents direct to the user's inbox, full portal-based pull encryption to manage encrypted messages entirely from a secure portal, and S/MIME to encrypt email messages and add a digital signature to safeguard against email spoofing.
		Sophos 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 Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.
		Sophos Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Sophos Firewall	The Sophos Cryptographic Module incorporated into the Sophos Firewall systems provides FIPS 140-2 validated cryptography for the protection of sensitive information.

No.	Security Requirements	Sophos Solution	How It Helps
3.13.13	Control and monitor the use of mobile code.	Sophos Mobile	Monitors mobile devices for jailbreaking and application sideloading. Denies access to email, network, and other resources if device is not in compliance with policy.
		Sophos Managed Detection and Response (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	Endpoint Protection application control policies restrict the use of unauthorized applications.
3.13.15	Protect the authenticity of communications sessions.	Sophos Email	Automatically scans message bodies and attachments for sensitive data, allowing you to easily establish policies to block or encrypt messages with just a few clicks. Sophos Email Offers TLS encryption and support for SMTP/S along with push-based encryption to send encrypted emails and attachments as password protected documents direct to the user's inbox, full portal-based pull encryption to manage encrypted messages entirely from a secure portal, and S/MIME to encrypt email messages and add a digital signature to safeguard against email spoofing.
		Sophos Cloud Optix	Establishes guardrails to prevent, detect, and remediate accidental or malicious changes in network configuration, network traffic, resource configuration, and user behavior or activities.
		Sophos Managed Detection and Response (MDR)	Sophos MDR continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events. Anomalous behaviors and code use are detected, investigated, and correlated to identify malicious activities and enable us to quickly neutralize the event.
		Sophos Firewall	With the Active Threat Response feature, it automatically coordinates a response with endpoints, wireless, ZTNA, email, and other Sophos solutions to stop threats dead in their tracks when a threat or indicator of compromise is detected. Dynamic firewall rules ensure that compromised devices are unable to communicate with command-and-control servers or move around the network.
		Sophos Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.
3.13.16	Protect the confidentiality of CUI at rest.	Sophos Firewall Sophos Intercept X Sophos Intercept X for Server	Data Leakage Prevention (DLP) capabilities in Sophos products can detect sensitive data and can prevent leaks of such information via email, uploads, and local copying.
		Sophos Managed Detection and Response (MDR)	24/7 monitoring of the environment plus investigation and neutralization of malicious activities secures against data loss through adversarial activities.
		Sophos 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.
		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.
		Sophos Mobile	A rich set of device management capabilities keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Flexible compliance rules monitor device health and flag deviation from desired settings.
		Sophos 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.

No.	Security Requirements	Sophos Solution	How It Helps
		Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
		Synchronized Security feature in Sophos products	Synchronized Security allows Sophos Firewall and Intercept X endpoint protection to work together to identify, isolate and clean up devices that have been compromised, preventing them from leaking confidential data. When the threat is neutralized and there is no risk of lateral movement, network connectivity is restored.
		Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
3.14 System and Information Integrity			
Basic Security Requirements			
3.14.1	Identify, report, and correct system flaws in a timely manner.	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 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 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.
3.14.2	Provide protection from malicious code at designated locations within organizational systems.	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.
		Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
		Sophos Managed Detection and Response (MDR)	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.

No.	Security Requirements	Sophos Solution	How It Helps
3.14.3	Monitor system security alerts and advisories and take action in response.	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
		Sophos Firewall	Integration with Sophos MDR and Sophos XDR allows Sophos Firewall to provide Automated Threat Response and Synchronized Security to stop threats before they can cause serious problem.
		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. 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.
		Sophos Network Detection and Response (NDR)	Continuously analyzes traffic for suspicious patterns and works with Sophos-managed endpoints and firewalls to monitor network activity for suspicious and malicious patterns. It detects abnormal traffic flows from unmanaged systems and IoT devices, rogue assets,insider threats, previously unseen zero-day attacks, and unusual patterns deep within the network. When an indicator of compromise, active threat, or adversary is detected, analysts are immediately alerted and can instantly push a threat feed to Sophos Firewall to trigger an automated response to isolate the compromised host.
		Sophos Managed Detection and Response (MDR)	Sophos MDR includes full incident response, delivered by a dedicated team of response specialists who are experts at battling adversaries. Clear procedures and documentation enable consistent info sharing.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
		Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
Derived Security Requirements			
3.14.4	Update malicious code protection mechanisms when new releases are available.	Sophos Intercept X Sophos Intercept X for Server	Intercept X continuously 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.
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		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 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 Network Detection and Response (NDR)	Continuously analyzes traffic for suspicious patterns. It detects abnormal traffic flows from unmanaged systems and IoT devices, rogue assets, insider threats, previously unseen zero-day attacks, and unusual patterns deep within the network.
		Sophos Managed Detection and Response (MDR)	Sophos MDR investigates suspicious signals, correlating data and behaviors and leveraging Sophos X-Ops threat intelligence for context and insights. On notification of vulnerabilities, Sophos MDR proactively hunts for exposure to enable swift remediation.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.

No.	Security Requirements	Sophos Solution	How It Helps
3.14.7	Identify unauthorized use of organizational systems.	Sophos Network Detection and Response (NDR)	Continuously analyzes traffic for suspicious patterns. It works with your managed endpoints and firewalls to monitor network activity for suspicious and malicious patterns that your endpoints and firewalls cannot see. It detects abnormal traffic flows from unmanaged systems and IoT devices, rogue assets,insider threats, previously unseen zero-day attacks, and unusual patterns deep within the network.
		Synchronized Security feature in Sophos products	Synchronized Security allows Sophos Firewall and Intercept X endpoint protection to work together to identify, isolate and clean up devices that have been compromised, preventing them from leaking confidential data. When the threat is neutralized and there is no risk of lateral movement, network connectivity is restored.
		Sophos 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.
		All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		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 XDR	Goes beyond the endpoint, pulling in rich network, email, cloud and mobile data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.
		Sophos Managed Detection and Response (MDR)	Sophos MDR investigates suspicious signals, correlating data and behaviors and leveraging Sophos X-Ops threat intelligence for context and insights. On notification of vulnerabilities, Sophos MDR proactively hunts for exposure to enable swift remediation.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.

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

2024-03-15 CC (MP)