SOPHOS

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 that store, transmit, or manage CUI. This document is based on the Federal Information Security Management Act of 2002 (FISMA) Moderate level requirements. It went into full effect on December 31, 2017.

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 XG Firewall Sophos SG UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group. Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos SD-RED [SD-WAN Remote Ethernet Devices] extends a secure network to a remote location easily by establishing a secure, dedicated VPN tunnel.
		Sophos SafeGuard Enterprise	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 Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location. Role-based administration assures user privacy and appropriate credentials for altering compliance or device/data access.
		Sophos Enterprise Console Sophos Central	Configurable role-based administration provides granular control of administrator privileges.
		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).

No.	Security Requirements	Sophos Solution	How it helps
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	Sophos XG Firewall Sophos SG UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group. Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos SD-RED [SD-WAN Remote Ethernet Devices] extends a secure network to a remote location easily by establishing a secure, dedicated VPN tunnel.
		Sophos SafeGuard Enterprise	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 Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.
	Derived Security Requirements		
3.1.3	Control the flow of CUI in accordance with approved authorizations.	Sophos XG Firewall Sophos SG UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group. Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos SD-RED [SD-WAN Remote Ethernet Devices] extends a secure network to a remote location easily by establishing a secure, dedicated VPN tunnel.
		Sophos Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.
		Sophos Central on Email Sophos XG Firewall Sophos SG UTM	Prevents messages containing sensitive data from leaving the organizations, with data loss prevention rules providing policy driven encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to help protect email content from unauthorized access.
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's assets.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Sophos Enterprise Console Sophos Central	Configurable role-based administration provides granular control of administrator privileges.
		Sophos Mobile	Role-based administration assures user privacy and appropriate credentials for altering compliance or device/data access.
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.

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 XG Firewall	Controls remote access authentication and user monitoring for remote access, and logs all access attempts.
		Sophos SafeGuard Enterprise	Provides detailed logging of 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.
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Sophos SafeGuard Enterprise	Encrypts data on Macs, Windows, and mobile devices. SafeGuard can manage BitLocker and FileVault full disk encryption, as well as always-on file encryption stored on hard disks, USB sticks, cloud storage, file shares, memory cards, and CDs/DVDs. All data encrypted with SafeGuard remains encrypted as files move across the network.
		Sophos Email on Central Sophos XG Firewall Sophos SG UTM	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 XG Firewall Sophos SG UTM	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos SD-RED [SD-WAN Remote Ethernet Devices] extends a secure network to a remote location easily by establishing a secure, dedicated VPN tunnel.
		Sophos Mobile	Encrypts documents within a secure container on a mobile device managed with Sophos Mobile. Sophos Secure Workspace can dynamically encrypt content sent to cloud-based storage services and applications. It enforces device encryption and monitors compliance relative to encryption policy.
		Sophos Wireless Sophos XG Firewall Sophos SG UTM	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.
3.1.17	Protect wireless access using authentication and encryption.	Sophos Wireless	When using our Security Heartbeat™ enabled APX Series access points, you can monitor the health status of any Sophos Central-managed endpoint or mobile device and automatically restrict web access on trusted Wi-Fi network. Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.	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 secures sensitive data with AES-256 encryption, allowing a secure way to manage, distribute, and edit documents and view web content on mobile devices.
3.1.21	Limit use of portable storage devices on external systems.	Sophos Intercept X Sophos Intercept X for Server	Device Control allows admins to control the use of removable media through policy settings.

No.	Security Requirements	Sophos Solution	How it helps
		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; access to latest know-how and expertise for security best practices.
		Sophos Phish Threat	Provides simulated phishing cyberattacks and security awareness training for the organization's end users. Courses cover a wide range of topics from phishing and cybersecurity overview lessons, through to data loss prevention, password protection and more.
	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, through to data loss prevention, password protection and more.
		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 Advanced with EDR	Detect, investigate, and respond to suspicious endpoint activity.
		Sophos XG Firewall	Controls remote access authentication and user monitoring for remote access, and logs all access attempts.
		Sophos SafeGuard Enterprise	Provides detailed logging of 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.
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.	Synchronized Security feature of Sophos Email and Sophos Phish Threat	Sophos Email 'At Risk Users' report highlights exactly which users are clicking email links re-written by Time-of-Click URL protection. Identifying users who have either been warned or blocked from visiting a website due to its risk profile. It's then simply one click from the report to enroll users in Phish Threat simulations and security awareness training – increasing their threat awareness and reducing risk.
		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 Intercept X Sophos Intercept X for Server	Get the 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 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.

No.	Security Requirements	Sophos Solution	How it helps
	Derived Security Requirements		
3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	All Sophos products	All administrative actions are logged and available for reporting and audits.
		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	Inventory management across multiple-cloud providers with continuous asset monitoring and complete network topology and traffic visualization.
	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 XG Firewall Sophos SG UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group.
		Sophos SafeGuard Enterprise	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 Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.
		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).
3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	Sophos XG Firewall Sophos SG UTM	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.
		Sophos Intercept X Sophos Intercept X for Server	HIPS, deep learning, anti-exploit, anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host.
		Sophos Mobile	Powered by deep learning protection, Sophos Mobile integrates with Sophos UTM, Sophos Wireless access points, and other UTMs to provide integrated and consistent security and compliance enforcement for mobile devices accessing the network and other services.

No.	Security Requirements	Sophos Solution	How it helps
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 XG Firewall Sophos SG UTM Sophos Web Gateway	Allows user-based policy control over applications, websites, categories, and traffic shaping (QoS). Synchronized Application Control in XG 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 to also apply traffic shaping.
		Sophos Intercept X	Endpoint Protection application control policies restrict the use of unauthorized applications.
		Sophos Intercept X for Server	Server Lockdown allows only trusted whitelisted applications and associated files to run.
3.4.9	Control and monitor user-installed software.	Sophos Mobile	Monitor devices for jailbreaking and side-loading of applications and deny access to email, network and other resources if device is not in compliance with policy.
		Sophos XG Firewall Sophos SG UTM	Visibility and Control over thousands of applications via customizable policy templates with granular controls based on category, risk, technology, or other undesirable characteristics (P2P apps, IMs, games and other harmful software); fully automated application security with pre-defined policy templates for commonly used enterprise applications / software packages; Synchronized Application Control in XG Firewall identifies all networked applications in the environment running on Sophos Managed Endpoints. Full list of controlled software / applications.
	3.5 Identification and Authentication		
	Basic Security Requirements		
3.5.1	Identify system users, processes acting on behalf of users, and devices.	Sophos XG Firewall Sophos SG UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group.
3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	Sophos XG Firewall Sophos SG UTM	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
		Sophos SafeGuard Enterprise	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 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).
		Sophos Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.

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 XG Firewall Sophos SG UTM	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
		Sophos SafeGuard Enterprise	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 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).
		Sophos Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.
	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. The Security Heartbeat also shares this information with Sophos Encryption, which revokes the encryption keys on the affected machine until the problem is fixed to prevent any data theft. After the systems have been automatically returned to their initial, clean state, the XG Firewall restores network access to the device, the encryption keys are returned, and your network is botnet-free.
		Sophos Email on Central Sophos XG Firewall Sophos SG UTM	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam.
		Sophos Intercept X Sophos Intercept X Advanced with EDR 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. Includes rollback to original files after a ransomware or Master Boot Record attack. Sophos Clean provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware.
		Sophos XG Firewall	Includes IPS, APT, antivirus, sandboxing with deep learning and web protection to monitor and block malicious, anomalous, and exploitive traffic from inbound or outbound access. Sophos Sandstorm, optional cloud-sandbox technology, inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.

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 Intercept X Advanced with EDR	Detects, investigates and responds to suspicious endpoint activity.
		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.
		Sophos SafeGuard Encryption	Provides complete data protection across multiple platforms and devices, including mobile devices; secures data at rest as well as in transit.
		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.
		3.9 Personnel Security	
	Basic Security Requirements		
3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	Sophos XG Firewall Sophos SG UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group.
		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).
		Sophos SafeGuard Encryption	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 Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.
3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers	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).

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.
		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 XG Firewall	Visibility and control over thousands of applications via customizable policy templates with granular controls based on category, risk, technology, or other undesirable characteristics (P2P apps, IMs, games and other harmful software); fully automated application security with pre-defined policy templates for commonly used enterprise applications / software packages; Synchronized Application Control in XG Firewall identifies all networked applications in the environment running on Sophos Managed Endpoints. View a full list of controlled software/applications.
		Sophos Mobile	Monitor mobile devices for jailbreaking and side-loading of applications Deny access to email, network, and other resources if device is not in compliance with policy.
		Sophos Intercept X Sophos Intercept X for Server	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. Server Lockdown allows only trusted whitelisted applications and associated files to run.
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. The Security Heartbeat also shares this information with Sophos Encryption, which revokes the encryption keys on the affected machine until the problem is fixed to prevent any data theft. After the systems have been automatically returned to their initial, clean state, the XG Firewall restores network access to the device, the encryption keys are returned, and your network is botnet-free.
		Sophos Intercept X Sophos Intercept X for Server	Includes rollback to original files after a ransomware or master boot record attack. Sophos Clean provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware.
		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	Intercept X consistently looks at reported false positives and false negatives to ensure the product is being continuously improved. It integrates a deep learning malware detection model that can scale to hundreds of millions of training samples and can 'memorize' the entire observable threat landscape as part of its training process. It is regularly trained by our SophosLabs team to stay up to date over time.

No.	Security Requirements	Sophos Solution	How it helps
		SophosLabs	Delivers the global threat intelligence advantage with Sophos' state-of-the-art big data analytics system that efficiently processes millions of emails, URLs, files, and other data points analyzed each day. This data, along with our extensive experience, enables us to develop new definitions, detect entire classes of threats, and even new variants. And, Live Protection and Live Anti-spam offer the data and expert analysis from SophosLabs in real time.
		3.13 System and Communications Protection	
	Basic Security Requirements		
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	Sophos XG 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. Allows for policy-based encryption for VPN tunnels, protecting data in transit.
		Sophos Mobile	Integration with Sophos UTM and other UTMs provides integrated and consistent security and compliance enforcement for mobile devices accessing the network and other services. Encrypts documents within a secure container on a mobile device managed with Sophos Mobile. Sophos Secure Workspace can dynamically encrypt content sent to cloud-based storage services and applications. It enforces device encryption and monitors compliance relative to encryption policy.
		Sophos Intercept X Sophos Intercept X for Server	HIPS, Deep Learning, Anti-exploit, Anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host.
		Sophos SafeGuard Enterprise	Encrypts data on Macs, Windows, and mobile devices. SafeGuard can manage BitLocker and FileVault full disk encryption, as well as always-on file encryption stored on hard disks, USB sticks, cloud storage, file shares, memory cards, and CDs/DVDs. All data encrypted with SafeGuard remains encrypted as files move across the network.
		Sophos Email on Central Sophos XG Firewall Sophos SG UTM	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.
	Derived Security Requirements		
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	Sophos Email	Sophos Email Content Control makes it easy to analyze email content and attachments for all inbound and outbound messages to ensure email data security.
3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Sophos XG 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.
		Sophos Mobile	Integration with Sophos UTM and other UTMs provides integrated and consistent security and compliance enforcement for mobile devices accessing the network and other services.

No.	Security Requirements	Sophos Solution	How it helps
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Sophos Email on Central Sophos XG Firewall Sophos SG UTM	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 Mobile	Encrypts documents within a secure container on a mobile device managed with Sophos Mobile. Sophos Secure Workspace can dynamically encrypt content sent to cloud-based storage services and applications. It enforces device encryption and monitors compliance relative to encryption policy.
		Sophos SafeGuard Enterprise	Encrypts data on Macs, Windows, and mobile devices. SafeGuard can manage BitLocker and FileVault full disk encryption, as well as always-on file encryption stored on hard disks, USB sticks, cloud storage, file shares, memory cards, and CDs/DVDs. All data encrypted with SafeGuard remains encrypted as files move across the network.
		Sophos XG Firewall Sophos SG UTM	Allows for policy-based encryption for VPN tunnels, protecting data in transit.
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Sophos SafeGuard Enterprise	Encrypts data on Macs, Windows, and mobile devices. SafeGuard can manage BitLocker and FileVault full disk encryption, as well as always-on file encryption stored on hard disks, USB sticks, cloud storage, file shares, memory cards, and CDs/DVDs. All data encrypted with SafeGuard remains encrypted as files move across the network.
		Sophos Central Device Encryption	Manages Windows BitLocker and macOS FileVault full disk encryption centrally from a single console. Web-based management eliminates the need to deploy a server or configure back-end key servers. Offers proof-of-compliance reporting to support your compliance efforts.
3.13.13	Control and monitor the use of mobile code.	Sophos XG Firewall	Visibility and control over thousands of applications via customizable policy templates with granular controls based on category, risk, technology, or other undesirable characteristics (P2P apps, IMs, games, and other harmful software); fully automated application security with pre-defined policy templates for commonly used enterprise applications/software packages; Synchronized Application Control in XG Firewall identifies all networked applications in the environment running on Sophos Managed Endpoints. View a full list of controlled software/applications.
		Sophos Mobile	Monitor mobile devices for jailbreaking and side-loading of applications. Deny access to email, network, and other resources if device is not in compliance with policy.
		Sophos Intercept X	Endpoint Protection application control policies restrict the use of unauthorized applications.
		Sophos Intercept X for Server	Server Lockdown allows only trusted whitelisted applications and associated files to run.

No.	Security Requirements	Sophos Solution	How it helps
3.13.15	Protect the authenticity of communications sessions.	Sophos Email on Central	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 Mobile	Encrypts documents within a secure container on a mobile device managed with Sophos Mobile. Sophos Secure Workspace can dynamically encrypt content sent to cloud-based storage services and applications. It enforces device encryption and monitors compliance relative to encryption policy.
		Sophos SafeGuard Encryption	Encrypts data on Macs, Windows, and mobile devices. Manages BitLocker and FileVault full disk encryption as well as always-on file encryption stored on hard disks, USB sticks, cloud storage, file shares, memory cards, and CDs/DVDs. All data encrypted remains encrypted as files move across the network.
3.13.16	Protect the confidentiality of CUI at rest.	Sophos XG Firewall Sophos SG UTM Sophos Intercept X Sophos Intercept X for Server	Data Leakage Prevention (DLP) capabilities in Sophos products can detect credit or debit card numbers and can prevent leaks of credit and debit card details via email, uploads, and local copying.
		Sophos Email on Central Sophos XG Firewall Sophos SG UTM	Leverages Sophos SPX encryption to dynamically encapsulate email content and attachments into a secure encrypted PDF.
		Sophos Mobile	Sophos Secure Workspace secures work documents with AES-256 encryption, allowing a secure way to manage, distribute, and edit business documents and view web content on mobile devices. 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.
		Sophos SafeGuard Encryption Sophos Central Device Encryption	Encrypts data on Macs, Windows, and mobile devices. Device Encryption provides centrally-managed, full disk encryption using Windows BitLocker and Mac FileVault. Sophos application-based (synchronized) encryption is automatic and always-on, i.e. content is encrypted as soon as it is created and it stays encrypted even when shared or uploaded to a cloud-based file-sharing system or removable devices. Role-based management is available to separate authorization levels and your encryption policies, keys, and self-service key recovery can be centrally managed.
	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.
		Synchronized Security feature of Sophos Email and Sophos Phish Threat	Sophos Email 'At Risk Users' report highlights exactly which users are clicking email links re-written by Time-of-Click URL protection. Identifying users who have either been warned or blocked from visiting a website due to its risk profile. It's then simply one click from the report to enroll users in Phish Threat simulations and security awareness training – increasing their threat awareness and reducing risk.

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. Includes rollback to original files after a ransomware or master boot record attack, along with Sophos Clean which provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware as well.
3.14.2	Provide protection from malicious code at designated locations within organizational systems.	Sophos Intercept X Sophos Intercept X for Server	Anti-exploit, anti-ransomware, and deep learning malware detection protect endpoints from malicious executable code.
		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 Email on Central Sophos XG Firewall Sophos SG UTM	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam.
		Sophos XG Firewall	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 Mobile	Delivers Unified Endpoint Management (UEM) and security management for mobile devices, helping ensure sensitive data is safe, devices are protected, and users are secure. Sophos Mobile Security for Android provides leading antivirus, ransomware, and unwanted app protection for Android devices.
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 Email on Central Sophos XG Firewall Sophos SG UTM	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam.
		Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect and remediate threats with ease. 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.
		Synchronized Security feature of Sophos Email and Sophos Phish Threat	Sophos Synchronized Security now connects Sophos Email with Sophos Endpoint. Delivering automatic detection and cleanup of infected computers sending outbound spam and viruses.
		Sophos XG Firewall	Includes IPS, APT, antivirus, sandboxing with deep learning, and web protection to monitor and block malicious, anomalous, and exploitive traffic from inbound or outbound access. Sophos Sandstorm, optional cloud-sandbox technology, inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.

NIST SP800-171

No.	Security Requirements	Sophos Solution	How it helps
	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.
3.14.7	Identify unauthorized use of organizational systems.	Sophos XG Firewall	Visibility and control over thousands of applications via customizable policy templates with granular controls based on category, risk, technology, or other undesirable characteristics (P2P apps, IMs, games and other harmful software); fully automated application security with pre-defined policy templates for commonly used enterprise applications / software packages; Synchronized Application Control in XG Firewall identifies all networked applications in the environment running on Sophos Managed Endpoints. View a full list of controlled software/applications.
		Sophos Mobile	Monitor mobile devices for jailbreaking and side-loading of applications. Deny access to email, network, and other resources if device is not in compliance with policy.
		Sophos Intercept X Sophos Intercept X for Server	Endpoint Protection application control policies restrict the use of unauthorized applications.
		Sophos Intercept X for Server	Server Lockdown allows only trusted whitelisted applications and associated files to run.

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

2020-04-10 CC (PC)

SOPHOS