PCI DSS v4.0 Compliance Reference Card

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. The standard covers all major areas of a security program in 12 sections in an effort to optimize the security of debit, credit and cash card transactions and to protect the misuse of personal information given by cardholders.

The PCI Security Standards Council (PCI SSC) issued version 4.0 of the PCI Data Security Standard (PCI DSS), replacing PCI DSS version 3.2.1, on March 31, 2022, to address emerging threats and technologies better and provide innovative ways to combat new threats. The existing version of PCI DSS v3.2.1 will be valid for two years until it is discontinued on March 31, 2024, to allow organizations time to grasp the changes in PCI DSS version 4.0 and apply the necessary changes adjustments. This document describes how Sophos solutions can be effective tools to help address some of the requirements as part of a customer's efforts to comply with PCI DSS.

Specifications and descriptions are subject to change without notice. Sophos disclaims all warranties and guarantees regarding this information. Use of Sophos products alone does not guarantee legal compliance. The information in this document does not constitute legal advice. Customers are solely responsible for compliance with all laws and regulations, and should consult their own legal counsel for advice regarding such compliance.

Requirement	Sophos Solution	How it helps
	Requirement 1: Install and maintain network security controls	
1.2 Network security controls (NSCs) are configured and maintained.	Sophos Firewall	Includes next-gen IPS that offers advanced protection from hacks and attacks using a uniform signature format backed by SophosLabs. Besides traditional servers and network resources, it also helps to identify and protect users and applications on the network. Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network Lateral Movement Protection, a Synchronized Security feature, is designed to prevent the threat or hacker from spreading to other systems, stealing data, or communicating back to the host.
	Sophos Intercept X Sophos Intercept X for Server	Enforces web, data, and device policies to allow only authorized applications to be run, devices to be connected and data to be distributed.
	Sophos 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 ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
	Sophos Managed Detection and Response (MDR)	Threat hunting experts monitor and correlate signals from across the network, identifying and investigating suspicious activities. Sophos NDR generates high caliber, actional signals across the network infrastructure to optimize cyber defenses.
	Sophos Rapid Response Service	Get fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.

Requirement	Sophos Solution	How it helps
1.3 Network access to and from the cardholder data environment is restricted.	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 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.
1.4 Network connections between trusted and untrusted networks are controlled.	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 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.
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.	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 Switch	Allows configuration of VLANs to segment your internal traffic and reduce the attack surface in case of an infection or breach.
	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 Intercept X Sophos Intercept X for Server	Enforces web, data, and device policies to allow only authorized applications to be run, devices to be connected and data to be distributed.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	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 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.

Requirement	Sophos Solution	How it helps
		Requirement 2: Apply secure configurations to all system components
2.2 System components are configured and managed securely.	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. Administrators are instructed to change the default password of the "admin" user immediately after deployment. An alert is displayed when the default password for the super administrator is not changed.
	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 Central	Disables or removes default passwords. Passwords are sufficiently complex to withstand targeted "brute force" attacks and must be rotated periodically. Keeps access lists and user privileges information up-to-date. Procedures are in place to revoke access rights if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
	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 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.
2.3 Wireless environments are configured and managed securely.	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.
		Requirement 3: Protect stored account data
3.5 Primary account number (PAN) is secured wherever it is stored.	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 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.
	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.

Requirement	Sophos Solution	How it helps
Requirement 4: Protect cardholder data with strong cryptography during transmission over open, public networks		
4.2 PAN is protected with strong cryptography during transmission.	Sophos Email	Encrypt messages and add a digital signature to verify sender identity with S/MIME, or select from customizable encryption options, including TLS encryption, attachment and message encryption (PDF and Office), or add-on full web portal encryption.
	Sophos Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos-managed networks and hotspots.
Requirement 5: Protect all systems and networks from malicious software		
5.2 Malicious software (malware) is prevented, or detected and addressed.	Sophos Firewall	Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Delivers advanced protection from the latest drive-by and targeted web malware, URL/Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
	Sophos Cloud Optix	Proactively identifies an 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..
	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	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 XDR	Detects and investigates across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
	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	Provides incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.

Requirement	Sophos Solution	How it helps
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.	Sophos Firewall	Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Delivers advanced protection from the latest drive-by and targeted web malware, URL/Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
	Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
	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	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 XDR	Detects and investigates across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
	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.
5.4 Anti-phishing mechanisms protect users against phishing attacks.	Sophos Email	Keeps phishing imposters out, automatically identifying your high-profile targets for malware-free impersonation and Business Email Compromise attacks. It then blocks the attack with machine learning analysis of message content, sender authentication, URL protection, and cloud sandboxing.
	Requirement 6: Develop and maintain secure systems and software	
6.2 Bespoke and custom software are developed securely.	Sophos Cloud Optix	DevSecOps tools work seamlessly with existing DevOps processes to help prevent security breaches pre-deployment. Sophos Cloud Optix scans container images in ECR, ACR, Docker Hub registries, as well as GitHub and Bitbucket IaC environments to identify operating system vulnerabilities and fixes to prevent threats pre-deployment. Prevents Infrastructure-as-Code (IaC) templates containing insecure configurations as well as embedded secrets and keys from never making it to a test or live production environment.
6.3 Security vulnerabilities are identified and addressed.	Sophos Firewall	Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Delivers advanced protection from the latest drive-by and targeted web malware, URL/Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
	Sophos Intercept X Sophos Intercept X for Server	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 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.
	Synchronized Security in Sophos products	Sophos Firewall with Security Heartbeat™ allows next-generation endpoint and network security to continuously share meaningful information about suspicious events across extended IT ecosystem; detects compromised / unauthorized endpoint device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.
	Sophos 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.

Requirement	Sophos Solution	How it helps
	Sophos XDR	Detect and investigate across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
	Sophos 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.
6.4 Public-facing web applications are protected against attacks.	Sophos Firewall	Combines next-gen firewall capabilities with our enterprise-class web application firewall to protect your critical business applications from hacks and attacks while still enabling authorized access.
	Sophos Cloud Optix	Sophos Web Application Firewall (WAF) protects your cloud workloads against hackers and offers reverse proxy authentication for secure user access.
6.5 Changes to all system components are managed securely.	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.
	All Sophos products	All administrative actions are logged and available for reporting and audits.
Requirement 7: Restrict access to cardholder data by business need-to-know		
7.2 Access to system components and data is appropriately defined and assigned.	Sophos Firewall	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling user-level access controls. Supports flexible multi-factor authentication options including directory services for access to key system areas.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	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 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 Central	Protects privileged and administrator accounts with advanced two-factor authentication. Configurable role-based administration provides granular control of administrator privileges. 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).

Requirement	Sophos Solution	How it helps
Requirement 8: Identify users and authenticate access to system components		
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.	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 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).
8.3 Strong authentication for users and administrators is established and managed.	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.
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.	Sophos Firewall	Supports flexible multi-factor authentication options including directory services for access to key system areas.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication.
	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.
8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse	Sophos Cloud Optix	Adopt the principle of least privilege across public cloud environments with Sophos Cloud Optix, Cloud Security posture Management solution. The SaaS based service connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real time to identify credential misuse or theft. It includes an IAM visualization tool that provides a complete map of IAM relationships and allows teams to quickly and easily identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Sophos Mobile	Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. A rich set of device management capabilities, containers, and market-leading encryption keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices.
	Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication.

Requirement	Sophos Solution	How it helps
	Requirement 10: Log and monitor all access to system components and cardholder data	
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
	Sophos XDR	Goes beyond the endpoint, pulling in rich network, email, cloud and mobile data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.
10.3 Audit logs are protected from destruction and unauthorized modifications.	Sophos Firewall	Stored logs cannot be accessed, destroyed, or altered without administrator privileges. To prevent accidental destruction due to destruction of firewall device altogether, the logs can be integrated into independent syslog server or into Sophos Central.
10.4 Audit logs are reviewed to identify anomalies or suspicious activity	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
	Sophos XDR	Goes beyond the endpoint, pulling in rich network, email, cloud and mobile data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.
	Sophos Managed Detection and Response (MDR)	Sophos MDR detects and investigates suspicious events from across the full security environment to identify threats and appropriate response activities. Data is collected across endpoint, network, identity email, and more, and then correlated using powerful AI tools, threat intelligence and human expertise to identify impact and response.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
10.5 Audit log history is retained and available for analysis.	Sophos Firewall	Sophos Firewall 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 into Sophos Central for analysis.
10.7 Failures of critical security control systems are detected, reported, and responded to promptly.	Sophos Firewall	Sophos Firewall can send alert notifications via Email or SNMP traps in case of failures of critical security controls. In addition, critical security failures can be highlighted on the Sophos Firewall dashboard or on Sophos Central Management and Reporting dashboard for immediate attention.
	Sophos Managed Detection and Response (MDR)	Collects data from Sophos Firewall to correlate using powerful AI tools, threat intelligence, and human expertise to identify impact and response.

Requirement	Sophos Solution	How it helps
	Requirement 11: Test security of systems and networks regularly	
11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.	Sophos Wireless	Automatically classifies neighboring networks to identify attempts to infiltrate an organization via Wi-Fi. An on-demand scan function shows you the very latest threat data.
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.	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.
	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	Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Delivers advanced protection from the latest drive-by and targeted web malware, URL/Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
	Sophos 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.
11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.	Security Consulting	Sophos offers penetration testing and vulnerability assessment of security infrastructure and software deployments; and recommendations for architecture and design changes needed to better use the available infrastructure.
	Sophos Cloud Optix	Cloud Optix allows security teams to focus on and fix their most critical public cloud security vulnerabilities before they are identified and exploited in cyberattacks. By identifying and risk-profiling security, compliance, and cloud spend risks, Cloud Optix enables teams to respond faster, providing contextual alerts that group affected resources with detailed remediation steps.
11.5 Network intrusions and unexpected file changes are detected and responded to.	Sophos Firewall	Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Delivers advanced protection from the latest drive-by and targeted web malware, URL/Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
	Synchronized Security feature in Sophos products	Sophos Firewall with Security Heartbeat™ allows next-generation endpoint and network security to continuously share meaningful information about suspicious events across extended IT ecosystem; detects compromised / unauthorized endpoint device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.
	Sophos 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)	Threat hunting experts monitor and correlate signals from across the network, identifying and investigating suspicious activities. Sophos NDR generates high caliber, actional signals across the network infrastructure to optimize cyber defenses.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.

Requirement	Sophos Solution	How it helps
		Requirement 12: Support information security with organizational policies and programs
12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.	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 Cloud Optix	Continually monitors public cloud resources, providing the visibility to proactively identify unsanctioned activity, vulnerabilities, and misconfigurations.
	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 Rapid Response Service	Provides incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	Sophos XDR	Detect and investigate across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
12.4 PCI DSS compliance is managed.	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. Continuously monitors compliance with custom or out-of-the box templates and audit-ready reports for standards such as PCI DSS, FFIEC, GDPR, HIPAA, and SOC2. Automatically analyzes cloud configuration settings against compliance and security best practice standards without diverting resources. Prevent compliance gaps leaving you exposed with a single view of compliance posture across AWS, Azure, and Google Cloud.
12.6 Security awareness education is an ongoing activity.	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.
12.7 Personnel are screened to reduce risks from insider threats.	Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication. Keeps access lists and user privileges information up to date.
	Sophos ZTNA	Constantly verifies the user — typically with multi-factor authentication and an identity provider — and validates health and compliance of the device for users to securely connect to corporate resources from any location.
	Sophos Email	Granular control of data breach prevention policies, including multi-rule policies for groups and individual users with seamless integration of encryption. Create custom CCLs using Sophos Content Control Lists or customize out of the box templates for specific CCLs. Choose from a variety of policy outcomes including block, drop attachment, quarantine as well as log and continue mode.
	Sophos Mobile	Encrypts documents within a secure container on a mobile device managed with Sophos Mobile. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.

Requirement	Sophos Solution	How it helps
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.	Sophos Intercept X with XDR	Provides comprehensive defense in depth against threats that get in via third party suppliers using AI, exploit prevention, behavioral protection, anti-ransomware and more. Plus, powerful XDR functionality enables you to automatically identify suspicious activity, prioritize threat indicators, and quickly search for potential threats across your endpoint and servers.
	Sophos Managed Detection and Response (MDR)	Delivers expert threat hunting and remediation as a fully-managed service. Sophos specialists work around the clock to proactively hunt for, validate, and remediate potential supply chain threats and incidents on your behalf.
	Sophos ZTNA	Safeguards against supply chain attacks that rely on supplier access to your systems via very granular access controls. This cloud-delivered solution validates user identity, and device health and compliance before granting access to resources. It authenticates requests from trusted partners, irrespective of the location.
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.	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 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 MDR swiftly contains and neutralizes incidents, with average time to detect, investigate and respond to just 38 minutes. Clients choose the level of response they wish us to take.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.

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

© Copyright 2022. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2022-12-06 RC (PS)

SOPHOS