
Executive Summary

Sophos Endpoint Security is deployed across the organization's endpoints to protect business systems and data against malware, ransomware, cyber threats, and unauthorized activities.

An annual **Sophos Endpoint Security Assessment** is conducted to evaluate the deployment, health status, security configurations, and effectiveness of endpoint protection controls. The assessment reviews endpoint coverage, security policies, protection settings, detections, alerts, and the overall endpoint security posture.

Where applicable, security controls such as **Threat Protection, Web Control, Application Control, Peripheral Control, Data Loss Prevention (DLP), Account Health Monitoring, and Tamper Protection** are reviewed to reduce cybersecurity risks, prevent unauthorized access, control the use of unauthorized applications and devices, and minimize the risk of data loss or leakage.

This assessment is benchmarked against **Sophos recommended security settings, Sophos Central Account Health Check, applicable CIS Critical Security Controls, and relevant PDPC ICT Security Guidance**, taking into consideration the organization's subscribed Sophos license, available security features, business requirements, and internal security policies. [\[docs.sophos.com\]](https://docs.sophos.com),

The objective of the assessment is to identify security gaps, validate the effectiveness of endpoint security controls, strengthen the organization's endpoint security posture, and provide documented evidence to support management review, cybersecurity governance, audit, and compliance activities.

IT SERVICE REPORT — SOPHOS ENDPOINT SECURITY ASSESSMENT

Document Version 2026

Date: 12 Jan 2026

Updated on 26 Aug 2026

Features	Explanation
Threat Protection	Protects endpoints against malware, ransomware, exploits, and malicious activities through real-time detection and automated response.
Peripheral Control	Controls removable media and external devices to reduce the risk of malware introduction and data leakage.
Application Control	Restricts the user of unauthorised, non-business, or high-risk application on managed devices.
Data Loss Prevention	Monitor sensitive information and prevent unauthorised disclosure of confidential data.
Web Control	Enforces safe browsing policies and blocks access to malicious, inappropriate, or high-risk websites.
Account Health	Enforces safe browsing policies and blocks access to malicious, inappropriate, or high-risk websites.
Tamper Protection	Enforces safe browsing policies and blocks access to malicious, inappropriate, or high-risk websites.

CUSTOMER INFORMATION		SERVICE INFORMATION	
Company Name		Commencement Date	
Contact Name		Completion Date	
Project Report No.		Engineer Name	

Assessment Objectives:

To evaluate the effectiveness of Sophos Endpoint Security controls and policies in protecting endpoints and organisational data against cyber threats, malware, ransomware, and data leakage, and to provide documented evidence supporting security governance, management review, audit, and compliance requirements.

Assessment Deliverables:

- a. Verify Sophos licensing, subscription status, endpoint deployment coverage, and policy assignment across all managed devices.
- b. Review Sophos Central Account Health, endpoint security posture, policy compliance, and protection status to identify unmanaged, outdated, or non-compliant endpoints.
- c. Assess Threat Protection configuration, including malware protection, ransomware protection, exploit prevention, Live Protection, Deep Learning, and endpoint isolation capabilities.
- d. Review Web Control, Application Control, Peripheral Control, and Data Loss Prevention (DLP) policies to verify they align with the organization's security requirements and regulatory obligations.
- e. Review security alerts, detections, incidents, exclusions, tamper protection status, and endpoint health indicators to identify potential security risks and misconfigurations.
- f. Evaluate compliance with applicable cybersecurity frameworks, industry best practices, and organizational security policies, including Sophos recommended settings, CIS Controls, and relevant regulatory requirements.
- g. Identify security gaps, policy exceptions, unsupported configurations, and areas for improvement, together with prioritized remediation recommendations.
- h. Document assessment findings, risk observations, configuration evidence, and management recommendations to support internal audits, compliance reviews, and management reporting.

Sophos Subscription Information:

Central Intercept X Advanced — 33 / 29 USED

License Number: D561348xxx

Customer Acceptance & Sign-Off

The assigned Entrust Network Engineer has completed the IT Security Assessment and scope of work stated above to my satisfaction.

We value your feedback and welcome any comments or suggestions to help us improve our services. Please contact us at helpdesk@entrustnetwork.com.

Customer Name	
Designation	
Co. Stamp & Signature	
Date & Time	

Kindly make a copy for customer reference.

Technical Documentation

I have reviewed and confirmed the IT setup in accordance with industry best practices and security guidelines.

Field	Details
Name of IT Engineer	
Date of Setup & Review	
Signature	

Supervisor Acknowledgment

Review and sign-off by the IT Director or IT Helpdesk Manager.

Field	Details
Name of IT Director / IT Helpdesk Manager	
Date of Assessment & Approval	
Signature of Supervisor	

Compliance Standards & References

This assessment supports endpoint security reviews, cybersecurity audits, and compliance initiatives by benchmarking the Sophos Endpoint Security deployment against recognised security standards, vendor best practices, and applicable regulatory requirements.

Standard	Reference Link
Sophos Central Admin Documentation	Validates endpoint security configurations against Sophos-recommended settings.
CIS Critical Security Controls	Provides recognised cybersecurity controls and best practices for endpoint protection.
PDPC ICT Security Guide	Supports protection of personal data through appropriate endpoint security measures.
Applicable Regulatory Requirements	Supports compliance with relevant frameworks such as ISO 27001, PDPA, MAS TRM, and sector-specific cybersecurity requirements.

Sophos Endpoint Security Assessment & Best Practice Checklist 2026

This checklist provides a structured framework for assessing Sophos Endpoint Security configurations and identifying opportunities to strengthen endpoint protection. The recommended settings serve as a security baseline only and should not be interpreted as mandatory compliance requirements.

Organizations should evaluate each control based on their industry sector, applicable regulations, subscribed Sophos features, security policies, operational requirements, and risk tolerance.

A — Threat Protection

Configure in: *My Products* → *Endpoint* → *Policies* → *Base Policy - Threat Protection* → *Settings tab*

No.	Threat Protection	Status
A1	Live Protection & Real-Time Scanning — Checks against Sophos Labs threat database to detect threats.	Enabled
A2	Deep Learning — To auto-detect threats, both new and unknown.	Enabled
A3	Remediation — Automatically cleans up malware and creates a Threat Graph creation.	Enabled
A4	Runtime Protection — Protects by detecting suspicious or malicious behaviour or traffic.	Enabled
A5	SSL/TLS Decryption of HTTPS Sites — Lets device decrypts and check content of HTTPS sites for threats (will slow down browsing).	Disabled
A6	Device Isolation — Devices will be isolated from the network if they report their health as red.	Enabled
A7	Scheduled Scanning — Performs a scan (legacy technique, increases system load and slows down significantly).	Disabled
A8	Exclusions	Disabled
A9	Desktop Messaging — Notifies you about threat protection events.	Enabled

B — Peripheral Control

Configure in: *My Products* → *Endpoint* → *Policies* → *Base Policy - Peripheral Control*

No.	Peripheral Control	Status
B1	Bluetooth	Enabled
B2	Optical Drive	Enabled
B3	Removable Storage	Enabled
B4	Wireless	Enabled
B5	MTP/PTP	Enabled

C — Application Control

Configure in: [My Products](#) → [Endpoint](#) → [Policies](#) → [Base Policy - Application Control](#)

No.	Application Control	Status
C1	Application Vulnerabilities	Blocked
C2	Archive Tool	Blocked (exception: 7-Zip, WinRAR, WinZip, NXPowerLite Desktop, PowerArchiver)
C3	Asset Management Tool	Allowed
C4	Browser Plug-In	Allowed
C5	Business Intelligence Tool	Allowed
C6	CRM Tool	Allowed
C7	Design Tool	Allowed
C8	Desktop Search Tool	Allowed
C9	Digital Imaging	Allowed
C10	Distributed Computing	Allowed
C11	Document Viewer	Allowed
C12	Download Manager	Blocked
C13	Email / PIM Client	Allowed
C14	Email Sync Tool	Allowed
C15	Encryption / Steganography Tool	Allowed
C16	ERP Software	Allowed
C17	File Sharing Application	Allowed
C18	FTP Client	Allowed
C19	Game	Blocked
C20	Instant Messaging	Allowed
C21	Internet Browser	Allowed
C22	Jailbreak Software	Blocked
C23	Mapping Application	Allowed
C24	Media Conversion Tool	Allowed
C25	Media Player	Allowed
C26	Mobile Synchronization	Allowed
C27	Network Monitor / Vulnerability Tool	Allowed
C28	Office Suite	Allowed
C29	Online Storage	Allowed
C30	Optical Burning Tool	Blocked
C31	Optical Media Emulation	Blocked
C32	Password / License Recovery Tool	Allowed

No.	Application Control	Status
C33	Pranking Software	Blocked
C34	Programming / Scripting	Allowed
C35	Privacy Tool	Blocked
C36	Proxy / VPN Tool	Allowed
C37	Remote Management Tool	Blocked (exception: Zoho Assist, TeamViewer, MS Remote Desktop Client, MS Remote Desktop Application, AnyDesk, iVMS 4200, LogMeIn for Mac, LogMeIn Server, 24x7 Site, Action1 Remote)
C38	Runtime Environment	Allowed
C39	Screen Capture Tool	Allowed
C40	Screensaver Application	Blocked
C41	Security Tool	Blocked
C42	Software Updater	Allowed
C43	System Tool	Allowed
C44	Telnet Client	Blocked (exception: PuTTY)
C45	Tethered Connection Tool	Allowed
C46	Toolbar	Allowed
C47	USB Program Launcher	Allowed
C48	Virtualization Application	Allowed
C49	Voice over IP	Allowed

D — Data Loss Protection

Configure in: [My Products](#) → [Endpoint](#) → [Policies](#) → [Base Policy - Data Loss Prevention](#)

No.	Data Loss Protection	Status
D1	Singapore Passport Number — Notifies the user if a passport number is detected.	Configured
D2	Singapore NRIC — Notifies the user if a Singapore NRIC is detected.	Configured
D3	Credit Card Number — Notifies the user if a credit card number is detected.	Configured

E — Web Control

Configure in: *My Products* → *Endpoint* → *Policies* → *Base Policy - Web Control*

No.	Web Control	Status
E1	Advertisements	Allowed
E1.1	Uncategorized	Warn
E1.2	Risky File Type	Block
E2	Productivity-related categories	Allowed (except gaming, gambling)
E2.1	Social Networking	Allowed
E2.2	Adult and Potentially Inappropriate Categories	Allowed (except Adult)
E2.3	Categories Likely to Cause Excessive Bandwidth Usage	Blocked (except media streaming)
E3	Protect Against Data Loss	Allowed
E4	Log Web Control Events	Enabled
E5	Control Sites Tagged in Website Management	Disabled
E6	Apply This Web Control Policy at Set Times Only	Disabled

F — Sophos Client Protection

Configure in: *My Products* → *Endpoint* → *Policies* → *Base Policy - Threat Protection* → *Tamper Protection* section

No.	Sophos Client Protection	Status
F1	Tamper Protection	Enabled

Supporting Evidence

The screenshots below provide evidence of the validity of the License subscription and the Threat Protection, Peripheral Control, Application Control, Data Loss Prevention, Web Control, Account Health, and Tamper Protection settings, all of which were reviewed and validated as part of this Sophos Endpoint Security Assessment.

1. Threat Protection

2. Peripheral Control

3. Application Control

4. Data Loss Prevention

5. Web Control

6. Account Health

2. Tamper Protection

End of Document | Sophos Endpoint Security Assessment | Version 2.0 | 2026
Confidential — Internal Use Only | Entrust Network Services Pte Ltd