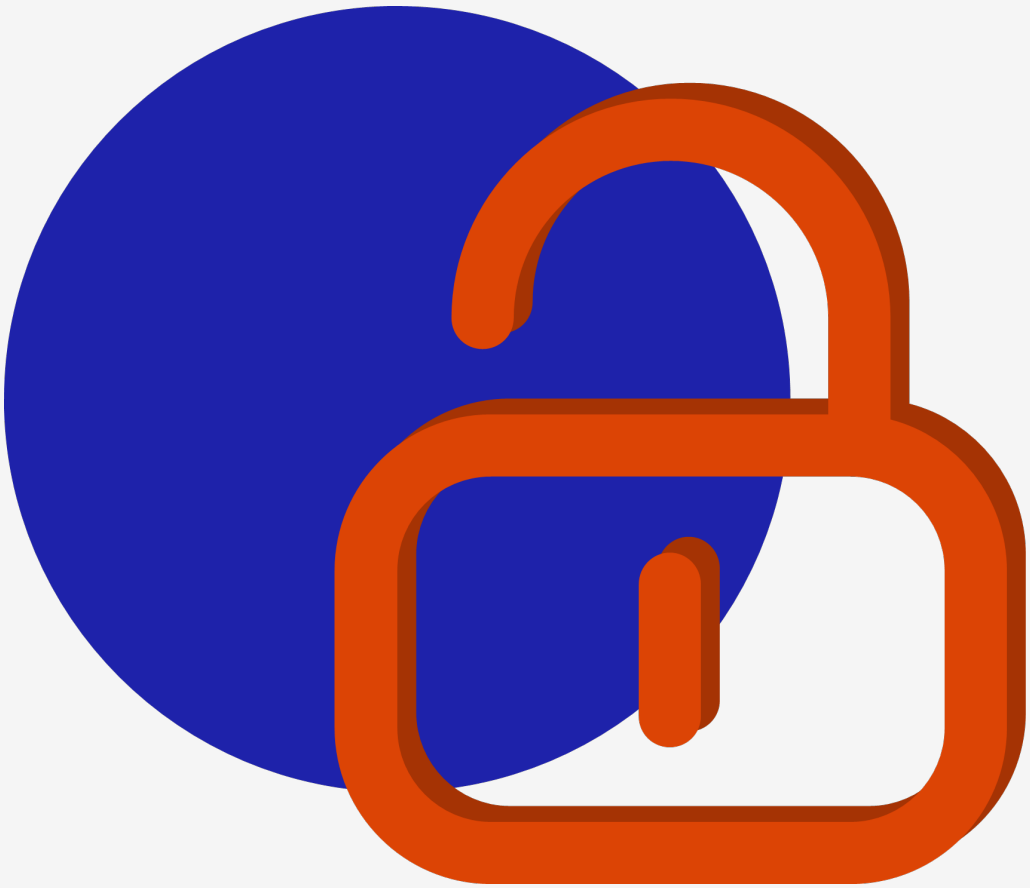
++

Sophos Endpoint Security Assessment: Letter of Attestation

Sophos

6 November 2025



MWR CYBERSEC

Document Control

Date	Change By	Change	Issue
2025–09–29	Christo Erasmus	Document created	0.1
2025–11–04	Andre Lopes	Document amended	0.1
2025–11–04	Connor du Plooy	Document amended	0.1
2025–11–04	Jacob Simmons	Document amended	0.1
2025–11–04	Matt Bouffé	Document amended	0.1
2025–11–04	Stephen Munro	Document amended	0.1
2025–11–04	Logan Kroeger	Document QA	0.2
2025–11–06	Christo Erasmus	Document published	1.0

Document Distribution

Date	Name	Company
2025–11–06	Steven Hedworth	Sophos

Contents

1. Overview

MWR CyberSec (MWR) conducted several security assessments against Sophos' endpoint security solutions for various operating systems. The scope of these security assessments was limited to identifying security vulnerabilities that could adversely affect a Sophos XDR agent or the endpoint on which an agent is installed on. These assessments did not include a *fitness-for-purpose* assessment to determine how well the agent functioned as Anti-Virus (AV) or Endpoint Detection and Response (EDR) solutions, and which Tactics, Techniques and Procedures (TTPs) could be used to bypass detection.

The platforms that were included for assessment in this project, as well as the specific components that were considered in-scope, are as follows:

- Sophos Intercept X Advanced with XDR – Windows
  - Scope:
    - Installation
    - Sophos AutoUpdate (SAU)
    - Sophos Clean / Clean-M
    - Central Device Encryption (CDE)
    - Time-boxed Tamper Protection assessment
  - Assessment Window:
    - Conducted from the 29th of September to the 29th of October, 2025
- Sophos Intercept X Advanced with XDR – macOS
  - Scope:
    - Tamper Protection controls and bypasses thereof
    - Sophos Service Manager
    - Installation, update and uninstallation processes
  - Assessment Window:
    - Conducted from the 29th of September to the 31st of October, 2025
- Sophos Protection for Linux (SPL) – Linux
  - Scope:
    - AV process termination for arbitrary process
    - AV process termination bypasses
    - Management Communications System (MCS) client
    - Communications between various plugins
  - Assessment Window:
    - Conducted from the 6th of October to the 4th of November, 2025

2. Approach

The sections below detail the high-level approach taken for the assessment of the Sophos endpoint agents on each platform. In general, a white-box approach was followed, with Sophos providing source code and detailed information regarding the in-scope components. The assessment consisted of practical testing against agents installed on test machines, assisted by source code reviews where appropriate.

2.1. Windows

The primary focus of the Windows component was to identify local privilege escalation vectors within the aforementioned in-scope components. The installation process was assessed to determine whether any misconfigurations or security weaknesses were introduced to the endpoint, that could result in privilege escalation. Any privileged file and registry operations performed by the installer, as well as the SAU and Sophos Clean components, were also reviewed for potential privilege escalation opportunities. The Central Device Encryption (CDE) component was reviewed in a time-boxed manner in attempts to identify security weaknesses or misconfigurations which may exist within this component, also with a focus on vulnerabilities that could lead to an escalation of privilege on the endpoint.

The Windows component also included a time-boxed review of the Sophos agent's Tamper Protection mechanisms. Within the available time, MWR attempted to identify any mechanisms that could allow an attacker to bypass or circumvent the agent's Tamper Protection controls.

2.2. macOS

Testing of the macOS Sophos endpoint solution focused on identifying weaknesses in the enhanced Tamper Protection functionality, installation procedures (including uninstall and update procedures), as well as specific Cross-Process Communication (XPC) services. As with the other components, source code was provided and MWR had the opportunity to engage and interact with Sophos developers to perform a time-limited source code review with the goal of identifying other misconfigurations.

2.3. Linux

The primary focus for assessing the Linux Sophos agent was the newly added process termination feature, specifically investigating if this new feature could be abused by an attacker to coerce the agent into terminating arbitrary processes, or if a malicious process could bypass the termination. Focus was also placed on the MCS client and its communication to the Sophos Central platform. Finally, inter-process communications was also investigated for any weaknesses in the communication between various plugins and components of the Linux Sophos agent.

3. Results

Robust security controls and a secure design were observed across the various platforms for the Sophos endpoint security agents assessed. The majority of the findings would not present significant risk to Sophos, or the endpoints on which they were installed, and remediation of these would serve to enhance the security posture of these endpoint agents. A summary of the vulnerabilities identified for each of the in-scope agents is noted in the table below, and subsequent sections thereof.

Assessment	HIGH	MEDIUM	LOW	INFORMATIONAL
Windows Endpoint Security Assessment	0	3	1	1
macOS Endpoint Security Assessment	0	1	2	2
Linux Endpoint Security Assessment	0	0	3	2
Total	0	4	6	5

Platform-Specific Commentary

Windows Agent

A total of 5 vulnerabilities were identified for the Sophos Windows endpoint agent, with 3 of these vulnerabilities being considered as medium-risk. One of the identified medium-risk vulnerabilities required administrative privileges on the endpoint, whilst the other 2 had a time-based restriction in which they could be exploited. Apart from the identified vulnerabilities, the Sophos Windows endpoint agent had a mature and securely implemented design for the in-scope components.

macOS Agent

Compared to the assessment performed in 2024 by MWR, two new vulnerabilities were discovered that presented an informational level of risk to Sophos, which if remediated, would further harden the security posture of the endpoint solution, and the endpoint on which it was installed. The tamper protection capability of the agent had also been improved since the previous assessment in 2024, and as such, recommendations for further improvement were made relating to this medium-risk vulnerability. The remaining findings pertained to hardening of inter-process communication mechanisms used by the agent, however these only presented low-risk to the endpoint on which the agent was installed.

Linux Agent

The Linux agent exhibited a total of five vulnerabilities, which were split between three low-risk and two informational-risk issues. The issues previously identified by MWR in 2024's assessment of the Linux endpoint agent were found to have been adequately remediated. The vulnerabilities identified in the 2025 assessment were largely related to defence-in-depth issues, or niche vulnerabilities with low exploitability or impact. As a result of this, the findings were found to exhibit a low-risk to Sophos or endpoints on which the agent was onboarded.

Overall Test Impressions

Recommendations on remediating the identified vulnerabilities and mechanisms for further hardening the security posture of the Sophos endpoint agents have been provided across all three platforms. The Sophos team was receptive to the findings and remedial actions, as well as being highly responsive and interactive throughout the course of the engagement.

Risk Rating Scale

The following risk profiles were used as guidelines to classify the vulnerabilities:

HIGH	A vulnerability will be assessed as representing a high risk if it holds the potential for an attacker to control, alter or delete Sophos' electronic assets. For example, a vulnerability which could allow an attacker to gain unauthorised access to a system or to sensitive data would be assessed as a high risk. Such issues could ultimately result in the defacement of a web site, the alteration of data held within a database or the capture of sensitive information such as account credentials or credit card information.
MEDIUM	A vulnerability will be assessed to represent a medium risk if it holds, when combined with other factors or issues, the potential for an attacker to control, alter or delete Sophos' electronic assets. For example, a vulnerability that could enable unauthorised access to be gained if a specific condition was met, or an unexpected change in configuration was to occur, would be rated as a medium risk.
LOW	A vulnerability will be assessed to represent a low risk if the likelihood or impact of exploitation is extremely low. For example, this could be an HTTPS configuration that allows weak ciphers or outdated protocols, or a CAPTCHA that can be solved programmatically.
INFORMATIONAL	A vulnerability will be assigned the informational classification when it cannot be exploited directly but is not in line with security best practice. Such a vulnerability could provide information that would facilitate research into an attack against the target system. For example, disclosure of the server type in an HTTP response.

APPENDIX I – Project Team

Assessment Team

Lead Consultant	Christo Erasmus
Additional Consultants	Andre Lopes Connor du Plooy Jacob Simmons Matt Bouffé Stephen Munro

Quality Assurance

QA Consultant	Logan Kroeger

Project Management

Delivery Manager	Catherine de Wet
Account Director	Gaylen Postiglioni

MWR CYBERSEC