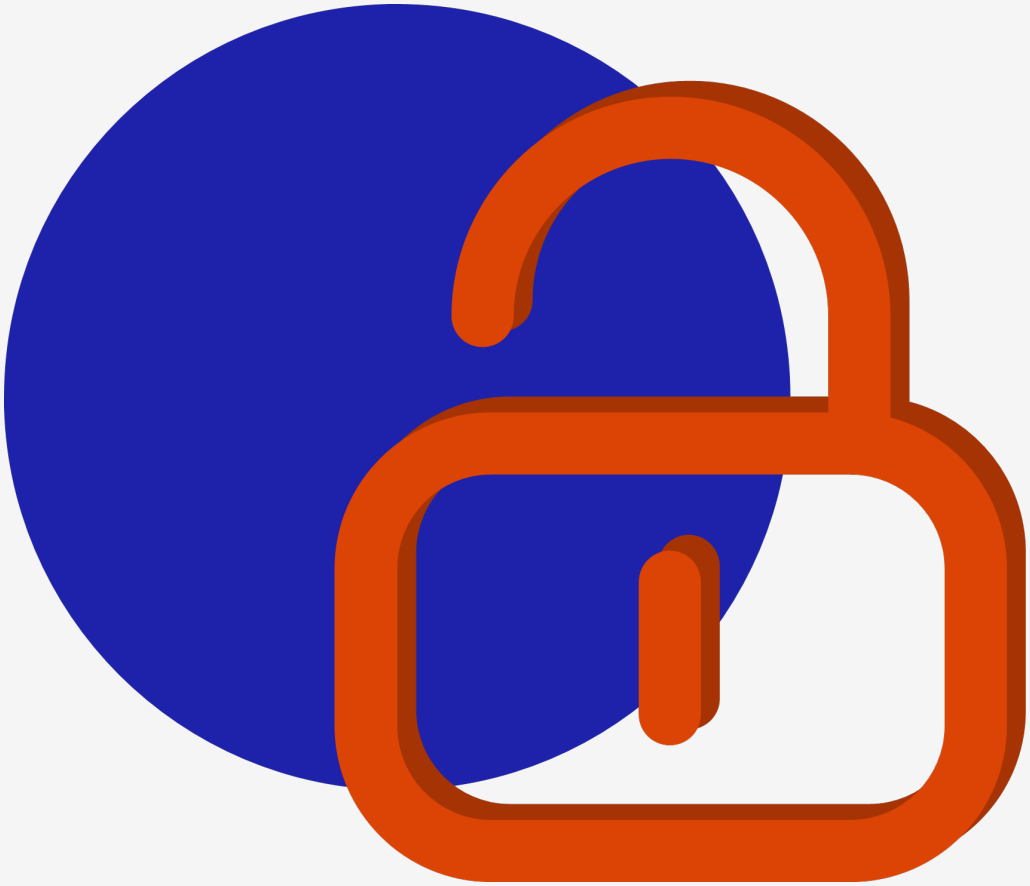
++

Sophos Central Security Assessment: Letter of Attestation

Sophos

27 February 2026



© MWR CyberSec

Document Control

Date	Change By	Change	Issue
2026–02–18	Ethan Havinga	Document created	0.1
2026–02–18	Oriana Karbownik	Document amended	0.1
2026–02–23	Jacob Simmons	Document amended	0.2
2026–02–23	Cheyenne De Beer	Document amended	0.2
2026–02–26	Robin Roodt	Document amended	0.3
2026–02–26	Daniel Mabasa	Document amended	0.3
2026–02–26	Matthew Bouffe	Document QA	0.4
2026–02–27	Ethan Havinga	Document published	1.0

Document Distribution

Date	Name	Company
2026–02–27	Sam Caise	Sophos

Contents

1. Overview

MWR CyberSec (MWR) conducted a security assessment of Sophos' Central environment. This consisted of the following three components:

- Sophos Central UI web application security assessment
- Sophos Central API security assessment
- AWS Security Configuration Review

Testing of the Sophos Central UI Web Application was conducted from the 30th January 2026 to the 26th of February 2026 and testing of the Sophos Central APIs was conducted from the 2nd February 2026 to the 24th of February 2026. The testing of both of these components was conducted in the production environment. The AWS security configuration review took place between the 23rd of January to the 3rd of February 2026 within the Sophos Central QA AWS account.

2. Approach

The scope of the assessment included an assessment of Sophos' Central Application UI application, Central APIs and an AWS Security Configuration Review.

Sophos Central Application UI and API Security Assessment

Testing of the Central application environment was conducted using MWR's security assessment methodology, which is in line with the CREST testing methodology, covering aspects such as information gathering, content discovery, injection attacks, and authentication and authorisation bypass attacks. The full testing methodology is available on request.

The testing consists of a series of phases that are performed in line with the activities that would be attempted by a real attacker. The approach allows an iterative process to be followed that enables information discovered at all phases of testing to be fed back into the process. This ensures a comprehensive assessment is performed in line with the operation of the Sophos' business and service delivery requirements.

The results of the test are then assessed based on input from the client and are interpreted within an appropriate business risk context. This ensures that an accurate assessment of the risks that are exposed can be conducted. Remedial actions can then be performed in line with their cost and the associated risks that will exist if not resolved.

AWS Security Configuration Review

An AWS security configuration review was performed by MWR on the Sophos Central QA AWS account, which mirrored the production environment. Testing was conducted using MWR's cloud security assessment methodology, which is a blended methodology conforming to several industry-standard frameworks and supplemented by MWR's own cloud security experience. This focused on (but was not limited to) cloud administration and patch management, network security controls, encryption at rest and in transit, identity and access management, resource access policies, certificate and secrets management, detection and audit controls, and AWS Cognito.

Using this approach, the configuration of Sophos's cloud environment was assessed and compared to security best-practices guidelines. MWR then identified security-relevant issues and assigned a risk rating based on the practical impact of misconfiguration abuse and the business context of the assessment.

3. Results

In total, 18 vulnerabilities were found during the course of the Central Security Assessment. The table below shows a count breakdown of these vulnerabilities per component and risk rating.

Assessment	HIGH	MEDIUM	LOW	INFORMATIONAL
Sophos Central API Security Assessment	1	0	1	1
Sophos Central UI Application Security Assessment	0	0	2	0
AWS Security Configuration Review	0	3	5	5
Total	1	3	8	6

Sophos Central UI Application Security Assessment

The overall security of Sophos Central UI Web Application was found to be of a high standard with the exception of two low-risk issues. These issues stemmed from defence-in-depth measures pertaining to input validation and configurations set on how the application handles exceptions.

Sophos Central API Security Assessment

The in-scope Sophos Central APIs demonstrated well architected technical security controls, and only one vulnerability was identified that posed a significant risk. Although this vulnerability was considered to be a high risk, only one instance out of the large number of endpoints was discovered. Overall, considering the size of the attack surface, the security posture of the Central APIs was of a high standard.

AWS Security Configuration Review

The Sophos AWS account assessed demonstrated mostly secure configurations, although some issues were identified. These issues stemmed from misconfigurations within identity and access management, but also included lower-risk misconfigurations which pertained to defense-in-depth and security best practices.

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's 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's 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	Ethan Havinga
Additional Consultants	Oriana Karbownik Jacob Simmons Robin Roodt Cheyenne De Beer Daniel Mabasa

Quality Assurance

QA Consultant	Matthew Bouffe

Project Management

Delivery Manager	Catherine de Wet
Account Director	Gaylen Postiglioni

MWR CYBERSEC