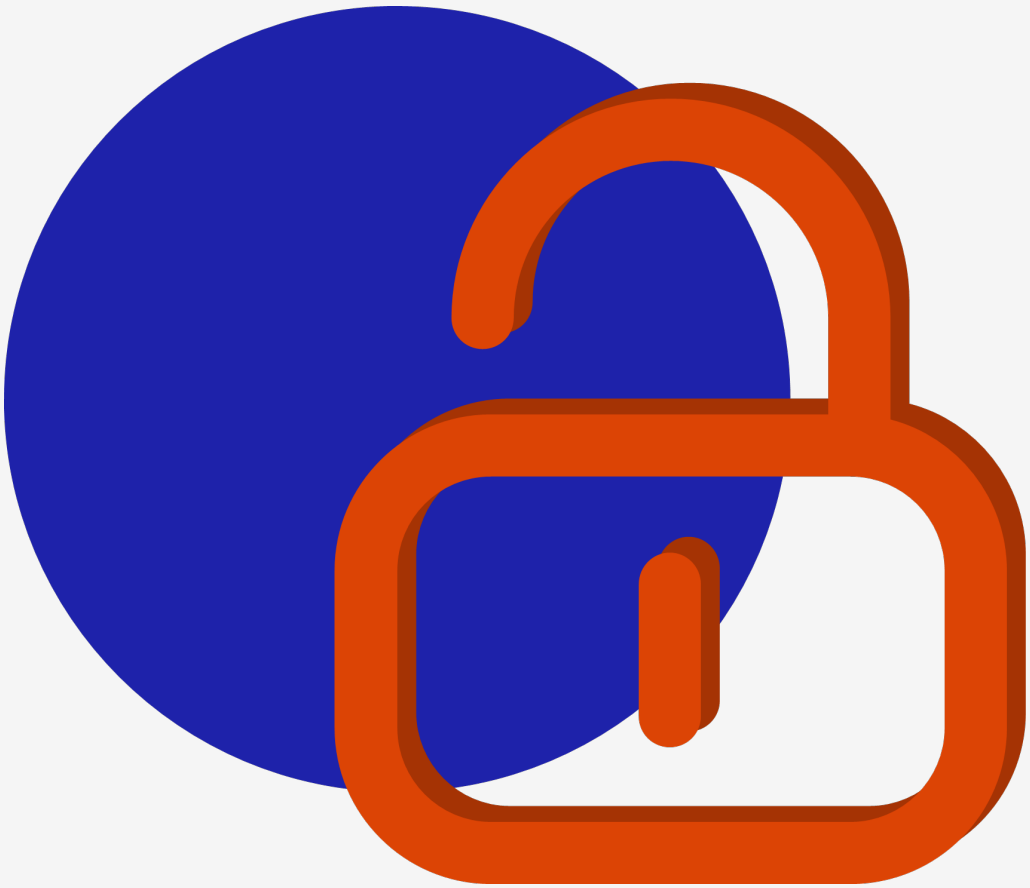
++

Taegis XDR Platform Security Review: Letter of Attestation

Sophos

17 November 2025



MWR CYBERSEC

Document Control

Date	Change By	Change	Issue
2025–11–06	Christopher Panayi	Document created	0.1
2025–11–17	Tinus Green	Document QA	0.2
2025–11–17	Christopher Panayi	Document published	1.0

Document Distribution

Date	Name	Company
2025–11–17	Steven Hedworth	Sophos
2025–11–17	Sam Caise	Sophos

1. Overview

MWR CyberSec (MWR) conducted a security assessment of the Taegis XDR platform from the 29th of July to the 8th of October 2025.

This assessment served as a broad security review of the XDR platform and its various components. The assessment was aimed at holistically assessing the platform's overall security posture. As the platform was in active use, Sophos' key motivation for testing was to ensuring that use of the solution did not introduce security risks to Sophos' or their clients' environments.

2. Approach

The scope of the assessment included timeboxed reviews of various platform components, which included:

- Taegis XDR Platform Authentication
- Taegis Endpoint Agent Authentication and associated APIs
- Taegis Endpoint Agent for Windows
- Taegis XDR Web Application and GraphQL APIs
- Taegis XDR Platform Data Ingestion APIs
- Taegis XDR Custom Query Language
- Taegis XDR Custom Playbooks

The components assessed during this project were considered representative of the feature set of the platform. The assessment followed a white-box approach, which allowed the MWR testing team to develop a good understanding of the implementation specific details of the platform. This was facilitated by access to the relevant source code, documentation, and members of the development team.

3. Results

Assessment	HIGH	MEDIUM	LOW	INFORMATIONAL
Taegis XDR Platform Authentication	2	2	1	0
Taegis XDR Web Application and GraphQL APIs	0	0	1	4
Taegis Endpoint Agent Authentication and APIs	0	1	1	0
Taegis Endpoint Agent for Windows	0	3	2	4
Taegis XDR Platform Data Ingestion APIs	0	0	0	0
Taegis XDR Custom Query Language	0	0	0	0
Taegis XDR Custom Playbooks	0	0	0	0
Total	2	6	5	8

Full access to all of the in-scope components was provided during testing. Close collaboration between MWR and the development team enabled the execution of in-depth targeted test cases against each component.

The high risk vulnerabilities identified during the assessment were remediated before the conclusion of the project and retesting of these vulnerabilities demonstrated that the remediations implemented were effective.

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	Christopher Panayi
Additional Consultants	Christo Erasmus Logan Kroeger Jacob Simmons Lian Aldrich

Quality Assurance

QA Consultants	Johan van der Merwe Sean Sproul Nick Brown Roy Fisher

Project Management

Delivery Manager	Jacqueline Isaac and Catherine de Wet
Account Director	Gaylen Postiglioni

MWR CYBERSEC