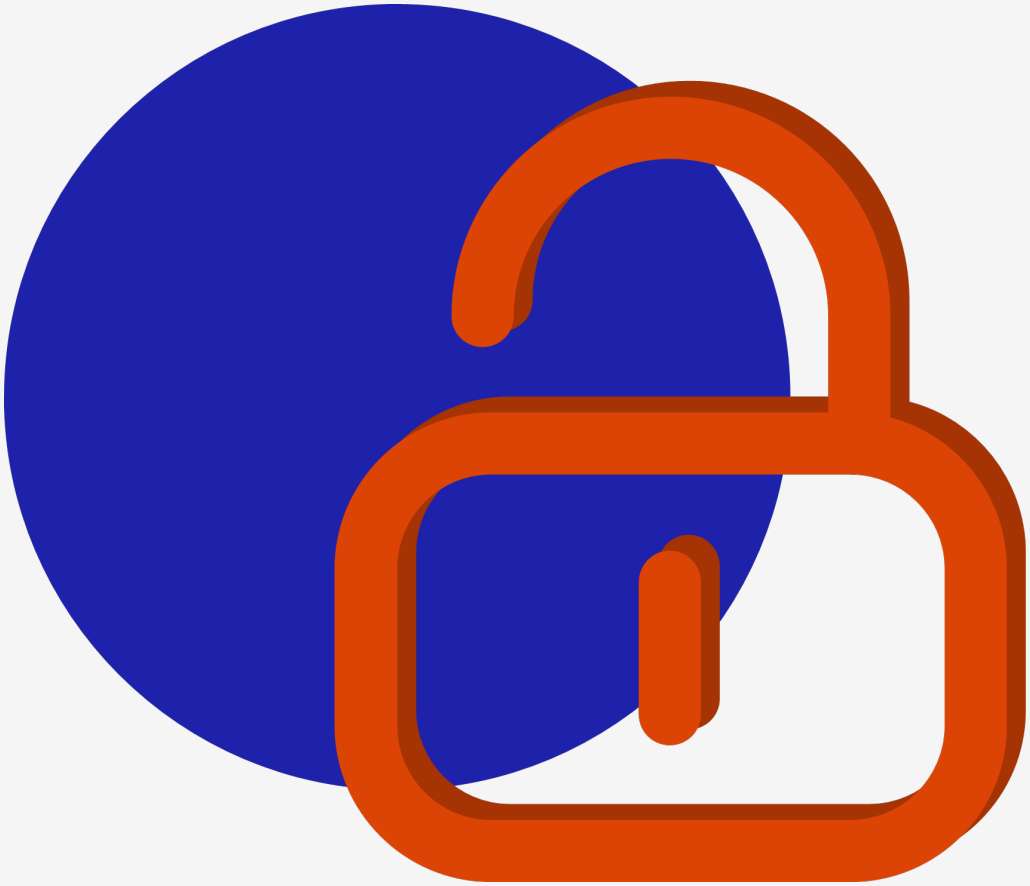
++

Sophos Taegis VDR Web Application Assessment Attestation Report

Sophos

22 July 2025



Document Control

Date	Change By	Change	Issue
2025–06–23	Lian Aldrich	Document created	0.1
2025–07–10	Cheyenne de Beer	Document amended	0.1
2025–07–10	Kevin Musengi	Document QA	0.2
2025–07–22	Lian Aldrich	Document published	1.0

Document Distribution

Date	Name	Company
2025–07–22	Steven Hedworth	Sophos

Contents

1 Overview 3
2 Approach 3
3 Results 4
Appendix I Disclaimer and Non-Disclosure Agreement 5
Appendix II Project Team 6

1. Overview

MWR CyberSec (MWR) conducted a security assessment of Sophos's Taegis VDR application. The Taegis VDR application was a cloud-based solution which allowed customers to manage assets and scan both internet-facing and internal assets for vulnerabilities. The application's primary functionality included managing assets, performing vulnerability scans on the assets, creating remediation plans, and managing user access. The application further included a public API which allowed tenants to expose their data to authenticated third parties.

Testing was performed on the following components that were considered in-scope:

- Taegis VDR Web Application:
  - Scope:
    - A security assessment of the VDR web application
    - This assessment covered the web application and underlying V1 API endpoints which the web application made use of
    - Focus was placed on authorisation controls to ensure that cross-client data access was not possible
  - Date:
    - Conducted from the 23rd of June to the 27th of June 2025
    - Continued from the 4th of July to the 10th of July 2025
- OpenAPI V2 API:
  - Scope:
    - A security assessment of the VDR V2 API
    - This assessment covered the accessible VDR V2 API endpoints which consisted of the following:
      - 103 Total Requests
      - 598 Total Parameters
  - Date:
    - Conducted from the 27th of June to the 3rd of July 2025

2. Approach

The assessment involved a comprehensive evaluation of the Taegis VDR application platform for web application and web service security vulnerabilities, with particular emphasis on testing controls that protect tenant information. The objective was to identify any weaknesses that could compromise the confidentiality, integrity, or availability of the platform, while placing specific focus on the enforcement of authorisation mechanisms.

To assess inter-tenant authorisation controls, testing was performed using two unrelated tenant accounts to determine whether data isolation between tenants was correctly enforced. This was done to ensure that users from one tenant could not gain unauthorised access to another tenant's information or functionality.

Intra-tenant authorisation controls were also evaluated by testing multiple user roles within the same tenant. This was conducted to verify that role-based access restrictions were properly implemented and that users could not perform actions or access data beyond their assigned privileges.

While authorisation controls were a key area of focus, testing also included a broader review of common web application vulnerabilities such as insecure API endpoints, input validation issues, and other weaknesses that could indirectly lead to unauthorised data access or compromise of the platform.

3. Results

The security posture of Taegis VDR application required improvement, as vulnerabilities were identified that could allow user accounts to be compromised, potentially leading to unauthorised access to sensitive data. This risk was introduced by the 1 high- and 2 medium-risk vulnerabilities identified through the assessment. The remaining low- and informational-risk vulnerabilities related to defense-in-depth measures that could be applied to further strengthen the secure posture of the Taegis VDR application platform. In total, 11 vulnerabilities were identified; the table below shows a count breakdown of these vulnerabilities per component and risk rating.

Assessment	HIGH	MEDIUM	LOW	INFORMATIONAL
Web Application Security Assessment	1	2	4	4
Total	1	2	4	4

The Taegis VDR application platform implemented strong authorisation controls which could not be bypassed to gain unauthorised access to information from a different tenant. The more significant vulnerabilities identified were isolated in nature and did not indicate systemic or pervasive design flaws.

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 – Disclaimer and Non-Disclosure Agreement

Non-Disclosure Statement

This report is the sole property of Sophos. All information obtained during the testing process is deemed privileged information and not for public dissemination. MWR CyberSec pledges its commitment that this information will remain strictly confidential. It will not be discussed or disclosed to any third party without the express written consent of Sophos. MWR CyberSec strives to maintain the highest level of ethical standards in its business practice.

Non-Disclosure Agreement

MWR CyberSec and Sophos have signed an NDA.

Disclaimer

This report is not meant as an exhaustive analysis of the level of security now present on the tested hosts, and the data shown here should not be used alone to judge security of any computer system. Some scans were performed automatically and may not reveal all the possible security holes present in the system. Some vulnerabilities that were found may be 'false positives', although reasonable attempts have been made to minimise that possibility. In accordance with the terms and conditions of the original quotation, in no event shall MWR CyberSec or its employees or representatives be liable for any damages whatsoever including direct, indirect, incidental, consequential loss or other damages.

APPENDIX II – Project Team

Assessment Team

Lead Consultant	Lian Aldrich
Additional Consultant	Cheyenne de Beer

Quality Assurance

QA Consultant	Kevin Musengi

Project Management

Delivery Manager	Jacqueline Isaac
Account Director	Gaylen Postiglioni

MWR CYBERSEC