

Certification Report

SolarWinds Hybrid Cloud Observability for Federal Government V2024.2.1

Sponsor and developer: **SolarWinds Worldwide, LLC**
7171 Southwest Parkway Building 400
Austin, Texas, 78735
USA

Evaluation facility: **UL**
De Heyderweg, 2
Leiden, 2314 XZ
The Netherlands

Report number: **NSCIB-CC-2300095-02-CR**

Report version: **1**

Project number: **NSCIB-2300095-02**

Author(s): **Brian Smithson**

Date: **16 April 2025**

Number of pages: **12**

Number of appendices: **0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

CONTENTS

Foreword	3
Recognition of the Certificate	4
International recognition	4
European recognition	4
1 Executive Summary	5
2 Certification Results	6
2.1 Identification of Target of Evaluation	6
2.2 Security Policy	6
2.3 Assumptions and Clarification of Scope	7
2.3.1 Assumptions	7
2.3.2 Clarification of scope	7
2.4 Architectural Information	7
2.5 Documentation	7
2.6 IT Product Testing	8
2.6.1 Testing approach and depth	8
2.6.2 Independent penetration testing	8
2.6.3 Test configuration	9
2.6.4 Test results	9
2.7 Reused Evaluation Results	10
2.8 Evaluated Configuration	10
2.9 Evaluation Results	10
2.10 Comments/Recommendations	10
3 Security Target	11
4 Definitions	11
5 Bibliography	12

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see <http://www.commoncriteriaportal.org>.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see <https://www.sogis.eu>.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the SolarWinds Hybrid Cloud Observability for Federal Government V2024.2.1. The developer of the SolarWinds Hybrid Cloud Observability for Federal Government V2024.2.1 is SolarWinds Worldwide, LLC located in Austin TX, USA and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a set of software applications and services executing on one or more Windows servers. The applications monitor a configured set of network-attached devices and applications for status, performance, and configuration settings. Depending on the size of the network, multiple instances of the applications may be deployed on different servers to provide adequate performance. For enhanced availability and robustness, a failover configuration may be deployed. SolarWinds Hybrid Cloud Observability for Federal Government V2024.2.1 consists of network, application, system, and storage monitoring components

The TOE was evaluated initially by UL located in Leiden, The Netherlands and was certified on 2024-04-18. The re-evaluation of the TOE has also been conducted by UL and was completed on 2025-04-16 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security [NSCIB].

The TOE had only minor changes from the previous evaluation:

- Updated module, component versions and installation file names.
- Updated guidance documentation references.
- Provided the updated website link for downloads.
- Updated supported browser versions

The certification took into account that the security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made, as well as renewed testing.

The scope of the evaluation is defined by the security target [ST], which identifies assumptions made during the evaluation, the intended environment for the SolarWinds Hybrid Cloud Observability for Federal Government V2024.2.1, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the SolarWinds Hybrid Cloud Observability for Federal Government V2024.2.1 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report [ETR]¹ for this product provide sufficient evidence that the TOE meets the EAL2 augmented (EAL2+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Flaw reporting procedures).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 [CEM] for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 [CC] (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

¹ The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the SolarWinds Hybrid Cloud Observability for Federal Government V2024.2.1 from SolarWinds Worldwide, LLC located in Austin TX, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	SolarWinds Platform Enterprise Operations Console (EOC) IP Address Manager (IPAM) Log Analyzer (LA) Network Configuration Manager (NCM) Network Performance Monitor (NPM) NetFlow Traffic Analyzer (NTA) Server & Application Monitor (SAM) Server Configuration Monitor (SCM) Storage Resource Monitor (SRM) User Device Tracker (UDT) Virtualization Manager (VMAN) VoIP & Network Quality Manager (VNQM) Web Performance Monitor (WPM)	V2024.2.1

To ensure secure usage a set of guidance documents is provided, together with the SolarWinds Hybrid Cloud Observability for Federal Government V2024.2.1. For details, see section 2.5 "Documentation" of this report.

2.2 Security Policy

Audit - Audit records are generated for specific actions performed by users. The audit records are stored in the SolarWinds database and may be viewed via the SolarWinds Web Console by authorized administrators.

Identification and Authentication – When a connection is established to the EOC Web Console or SolarWinds Web Console, the TOE prompts the user for login credentials. The credentials are validated by the TOE for the SolarWinds Web Console. For the EOC Web Console, the credentials are first passed to Windows for validation.

Management – The TOE offers a comprehensive set of management functions to reduce the likelihood of damage resulting from users abusing their authority by taking actions outside their assigned functional responsibilities. There are different TOE security function data for different TOE components, such as specific for NCM, IPAM and SCM etc. The management functionality provides multiple management access mechanisms for users. For each specific TOE security function data, dedicated access table will be established, the security function data privileges for the users vary based upon the definition. Individual user's access right for each TOE component security function data is determined by the user's role of each TOE component.

Network Monitoring – The status and performance of managed elements are monitored to enhance security and detect any potential threats to the managed systems. The results are saved and may be viewed by authorized users. Access to data about the managed elements may be limited by view limitations. Alerts may be generated to notify network managers of configured conditions detected about the managed elements. Conditions detected by HCO include element status changes and performance threshold values being exceeded.

Network Configuration Management – The configurations of network devices may be downloaded from the network device, saved in the TOE database, and compared to a reference configuration to



detect any potential threats to the managed network devices. If a configuration change is detected, an upload of a saved configuration for the network device may be triggered.

Server Configuration Management – The configurations of servers, windows registry, and applications may be collected via SolarWinds Agent, saved in the TOE database, and compared to a reference configuration to detect any potential threats to the managed devices.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

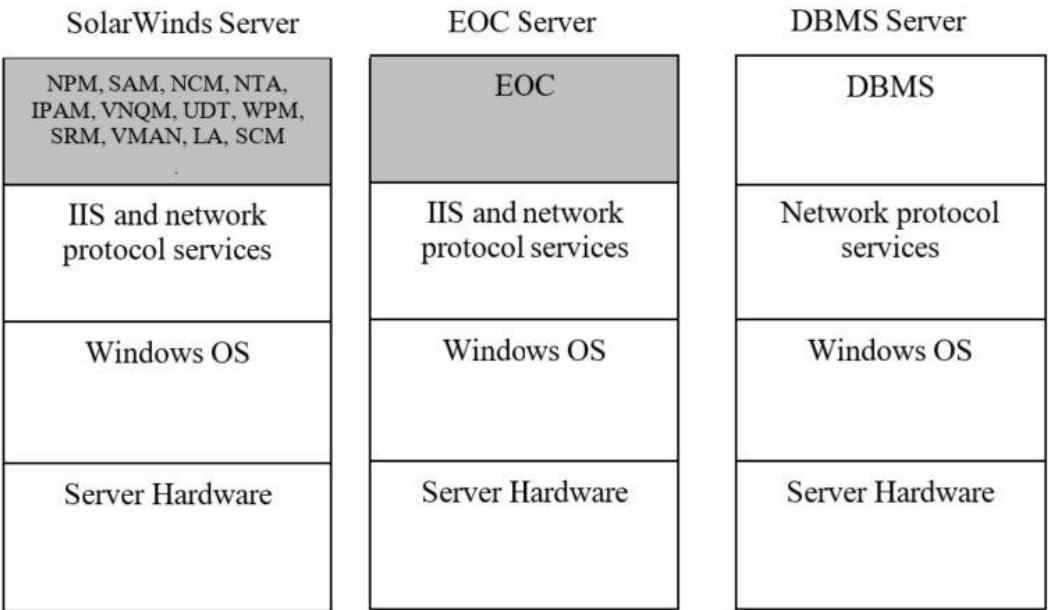
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 1.5.3 of the [ST].

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The TOE consists of the SolarWinds components identified in Section 2.1 executing on multiple dedicated Windows servers. The TOE is depicted in the figure below, with TOE components shaded. The operating systems (including the network protocol stacks and cryptographic functionality), web servers, and DBMS are outside the TOE boundary.



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
SolarWinds® Hybrid Cloud Observability for Federal Government Version 2024.2.1 Common Criteria Supplement	Version 1.1
SolarWinds® Platform Administrator Guide SolarWinds® Enterprise Operations Console Administrator Guide SolarWinds® Network Performance Monitor Administrator Guide	Version 2024.2

SolarWinds® Server & Application Monitor Administrator Guide SolarWinds® Network Configuration Manager Administrator Guide SolarWinds® IP Address Manager Administrator Guide SolarWinds® NetFlow Traffic Analyzer Administrator Guide SolarWinds® User Device Tracker Administrator Guide SolarWinds® VoIP and Network Quality Manager Administrator Guide SolarWinds® Log Analyzer Administrator Guide SolarWinds® Web Performance Monitor Administrator Guide SolarWinds Server Configuration Monitor Administrator Guide SolarWinds Storage Resource Monitor Administrator Guide Version SolarWinds® Virtualization Manager Administrator Guide	
---	--

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer tests have been chosen to represent a comprehensive set of essential functionality for the TOE. These tests cover adding, discovery, and management of nodes monitored by different protocols (SNMP, WMI, ICMP, Syslog, NetFlow, SMI-S), NCM configuration management functionalities, application monitoring, restrictions enforced by account permissions and roles, sites data aggregation in EOC.

The main purpose of the TOE is to monitor an IT environment (e.g., network, systems, storage, applications and databases) for issues, identify notable events/metrics/changes of interest based on configured policy, and ultimately alert administrators of problems, the developer test plan covers those kinds of essential functions.

Developer provided these evidence documents representing the developer testing effort;

- Test Plan giving an overview of the test environment configuration and requirements,
- Test Procedures containing step by step test scenarios and
- Test Results contains results of the conducted tests as described in the plan.

The test procedures document contains total of 16 developer test procedures. The test procedures are comprehensively testing most of the essential functionality of the TOE components by end-to-end design testing approach. Most of the test outputs are input to another test procedure like a chain of tests, each test is dependent to another test.

The evaluator concluded that the testing approach is adequate for this assurance level since all the TSFIs are covered extensively, and all the interactions between subsystems are exercised.

The evaluator analysed the coverage of the developer tests and sought to increase the percentage of TSFI, subsystem and SFR coverage of the developer and increased the coverage for all three dimensions. Especially for TSFIs and SFRs reached 100% coverage.

All developer tests were repeated by the evaluator. Developer's testing approach is based on testing all of the TOE components in a sequence. Almost all tests are dependent to at least one test case to be able to conduct the test. Developer test procedures comprehensively test most of the functionalities of the TOE.

The evaluator achieved its coverage goal by alternating the developer test procedures by different parameters, targeting missing subsystems, SFRs and TSFIs by adding new test scenarios and by reviewing documents to see if any test case is necessary based on the information gathered from through developer documents.

2.6.2 Independent penetration testing

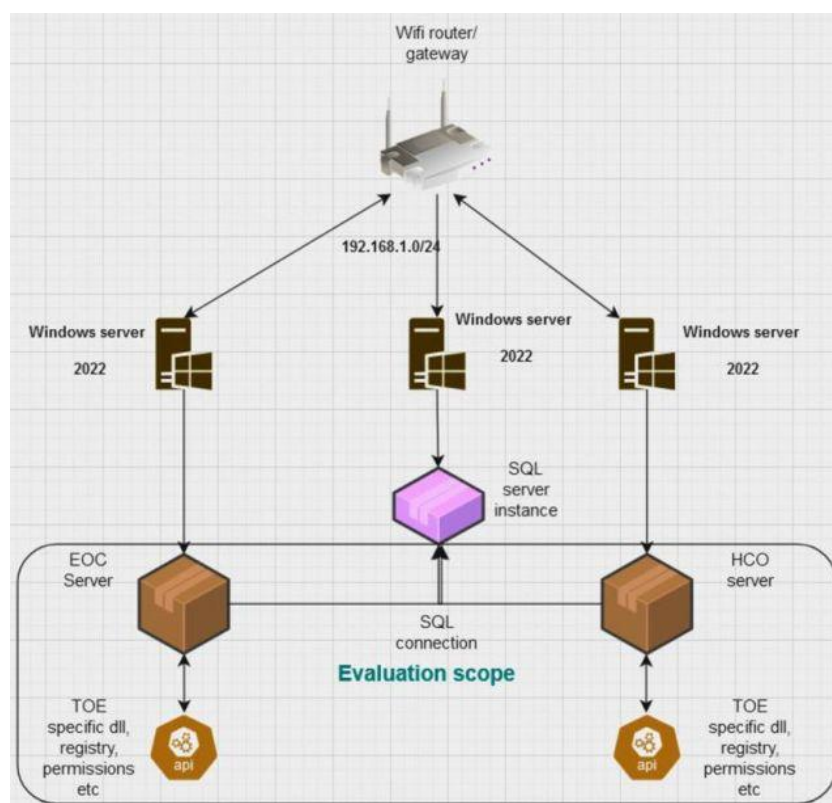
The evaluator performed a vulnerability analysis using a vulnerability-centric approach.

The test plan is derived from the analysis in [AVA-Pres], which includes the rationale for selection of vulnerabilities for penetration testing. The evaluator first installed the TOE in its optimal environment according to customer provided recommendations, then understanding how the product works, the configuration, items in scope of evaluation. Evaluator took time to configure the product, replicating a small network and getting data from different nodes. Evaluator then performed a simple threat modelling exercise to understand the different attack surface of the product. After performing these activities, evaluator started OSINT on the product to check for known vulnerabilities in the product, while understanding the product, evaluator noticed that it will be possible to get access to the some of the source code and third-party packages being used by the TOE, which will expand the attack surface without extensive effort. This analysis resulted into several test cases and the evaluator expects to uncover more test cases when penetration test starts.

The laboratory has dedicated a total of 25 man/day for the performance of AVA activities. These activities include a total of 15 relevant tests.

2.6.3 Test configuration

All of the penetration testing was performed on operational samples containing the final version of the TOE.



2.6.4 Test results

The SolarWinds Hybrid Cloud Observability for Federal Government TOE was evaluated against the Evaluation Assurance Level EAL2 augmented by ALC_FLR.2., as claimed in the Security Target [ST].

The evaluator concluded that the requirements of EAL2 augmented by ALC_FLR.2. have been met by the TOE and the associated evaluation evidence. The conclusion was drawn by conducting the associated evaluation activities specified in [CEM].

All potential vulnerabilities were found to be *Not Exploitable* by attackers having a VAN.2: Basic attack potential, thus the TOE in its evaluated configuration is compliant to the claimed level of assurance.

2.7 Reused Evaluation Results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been reused, but vulnerability analysis and penetration testing has been renewed.

No sites have been visited or are required as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number SolarWinds Hybrid Cloud Observability for Federal Government V2024.2.1. This is further enumerated by the component versions detailed in "Identification of Target of Evaluation", section 2.1 above.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the [ETR], which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "Pass".

Based on the above evaluation results the evaluation lab concluded the SolarWinds Hybrid Cloud Observability for Federal Government V2024.2.1, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL2 augmented with ALC_FLR.2**. This implies that the product satisfies the security requirements specified in Security Target [ST].

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: (none), which are out of scope as there are no security claims relating to these.

3 Security Target

The SolarWinds Hybrid Cloud Observability Software Security Target, v1.4, 3 March 2025 [ST] is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

DBMS	Database Management System
EOC	SolarWinds Enterprise Operations Console™
HCO	Hybrid Cloud Observability
IIS	Internet Information Services
IPAM	SolarWinds IP Address Manager™
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
LA	SolarWinds Log Analyzer™
NCM	SolarWinds Network Configuration Manager™
NPM	SolarWinds Network Performance Monitor™
NSCIB	Netherlands Scheme for Certification in the area of IT Security
NTA	SolarWinds NetFlow Traffic Analyzer™
NSCIB	Netherlands Scheme for Certification in the area of IT Security
OSINT	Open source intelligence
PP	Protection Profile
SAM	SolarWinds Server & Application Monitor™
SCM	SolarWinds Server Configuration Monitor™
SNMP	Simple Network Management Protocol
SRM	SolarWinds Storage Resource Monitor™
TOE	Target of Evaluation
UDT	SolarWinds User Device Tracker™
VMAN	SolarWinds Virtualization Manager™
VNQM	SolarWinds VoIP & Network Quality Manager™
WPM	SolarWinds Web Performance Monitor™

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[ETR]	SolarWinds Hybrid Cloud Observability for Federal Government Evaluation Technical Report, UL15390658/ETR, v2.0, 27 March 2025
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	SolarWinds Hybrid Cloud Observability Software Security Target, v1.4, 3 March 2025

(This is the end of this report.)