Certification Report

SolarWinds Orion Suite for Federal Government V4.1

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

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

Report number:	**NSCIB-CC-0036280-CR**
Report version:	**1**
Project number:	**0036280**
Author(s):	**Denise Cater**
Date:	**02 August 2021**
Number of pages:	**12**
Number of appendices:	**0**

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

Version 2021-3

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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, TÜV Rheinland Nederland 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 TÜV Rheinland Nederland 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 TÜV Rheinland Nederland 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, TÜV Rheinland Nederland 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.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement 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 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. The current list of signatory nations and approved certification schemes can be found at: http://www.commoncriteriaportal.org.

European recognition

The European SOG-IS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 effective since April 2010 provides mutual recognition 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 SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found at: http://www.sogisportal.eu.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the SolarWinds Orion Suite for Federal Government V4.1. The developer of the SolarWinds Orion Suite for Federal Government V4.1 is SolarWinds Worldwide, LLC located in Austin, 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.

TOE is a set of software applications (consists of 14 TOE components as stated in *[ST]*, section 1.2) that are able to perform network management functionalities such as network-attached devices and applications monitoring, configuration settings, device tracker, network performance management executing on one or more Windows servers.

The TOE has been evaluated by UL located in Leiden, The Netherlands. The evaluation was completed on 02 August 2021 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

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 Orion Suite for Federal Government V4.1, 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 Orion Suite for Federal Government V4.1 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 and *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland 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 releasable for public review.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the SolarWinds Orion Suite for Federal Government V4.1 from SolarWinds Worldwide, LLC located in Austin, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	SolarWinds Orion Suite for Federal Government V4.1, comprised of:	V4.1
	• SolarWinds Orion Platform	V2019.2 HF4
	• Enterprise Operations Console (EOC)	V2.2
	• IP Address Manager (IPAM)	V4.9
	• Log Analyzer (LA)	V2.1
	• Network Configuration Manager (NCM)	V8.0
	• Network Performance Monitor (NPM)	V12.5
	• NetFlow Traffic Analyzer (NTA)	V4.6
	• Server & Application Monitor (SAM),	V6.9.1
	• Server Configuration Monitor (SCM)	V1.2
	• Storage Resource Monitor (SRM)	V6.9
	• User Device Tracker (UDT)	V3.4
	• Virtualization Manager (VMAN)	V8.5
	• VoIP & Network Quality Manager (VNQM)	V4.6
	• Web Performance Monitor (WPM)	V3.0

To ensure secure usage a set of guidance documents is provided, together with the SolarWinds Orion Suite for Federal Government V4.1. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE provides the following security functionality:

- Audit - Audit records are generated for specific actions performed by users. The audit records are stored in the Orion database and may be viewed via the Orion Web Console by authorized administrators.
- Identification and Authentication – When a connection is established to the EOC Web Console or Orion Web Console, the TOE prompts the user for login credentials. The credentials are validated by the TOE for the Orion Web Console. For the EOC Web Console, the credentials are first passed to Windows for validation.
- Management – 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, dedicate 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. 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 Orion include element status changes and performance threshold values being exceeded.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

- 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. 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 Orion Agent, saved in the TOE database, and compared to a reference configuration.

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 4.2 of the *[ST]*.

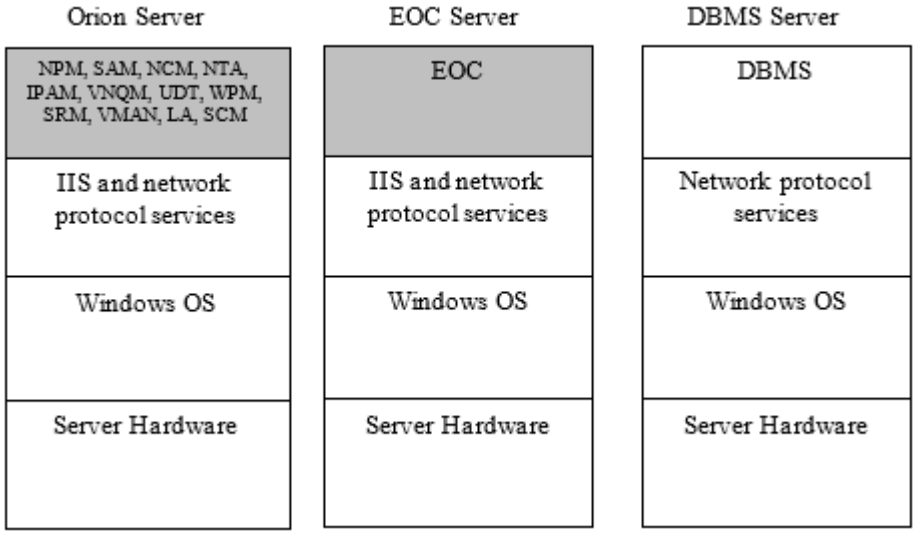
2.3.2 Clarification of scope

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

SolarWinds Orion Suite for Federal Government V4.1 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. The TOE consists of fourteen network, application, system, and storage monitoring components, as specified in *[ST]* section 1.5.

The following figure shows the TOE components in grey shading.



2.5 Documentation

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

Identifier	Version
SolarWinds® Orion® Suite for Federal Government Version 4.1 Common Criteria Supplement (OrionCommonCriteriaSupplement.pdf)	Version 2.5

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

SolarWinds® Enterprise Operations Console Getting Started (EOCv22AdministratorGuide.pdf)	Version 2.2
SolarWinds® Network Performance Monitor Administrator Guide (NPMv125AdministratorGuide.pdf)	Version 12.5
SolarWinds® Server & Application Monitor Administrator Guide (SAMv69AdministratorGuide.pdf)	Version 6.9.1
SolarWinds® Network Configuration Manager Administrator Guide (NCMv80AdministratorGuide.pdf)	Version 8.0
SolarWinds® IP Address Manager Administrator Guide (IPAMv49AdministratorGuide.pdf)	Version 4.9
SolarWinds® NetFlow Traffic Analyzer Administrator Guide (NTAv46AdministrationGuide.pdf)	Version 4.6
SolarWinds® User Device Tracker Administrator Guide (UDTv34AdministratorGuide.pdf)	Version 3.4
SolarWinds® VoIP and Network Quality Manager Administrator Guide (VNQMv46AdministratorGuide.pdf)	Version 4.6
SolarWinds® Log Analyzer Administrator Guide (LAv21AdministrationGuide.pdf)	Version 2.1
SolarWinds® Web Performance Monitor Administrator Guide (WPMv30AdministratorGuide.pdf)	Version 3.0
SolarWinds Server Configuration Monitor Administrator Guide (SCMv12AdministratorGuide.pdf)	Version 1.2
SolarWinds Storage Resource Monitor Administrator Guide (SRMv69AdministratorGuide.pdf)	Version 6.9
SolarWinds® Virtualization Manager Administrator Guide (VMANv85AdministratorGuide.pdf)	Version 8.5
SolarWinds® Server & Application Monitor Getting Started Guide (SAMv69GettingStartedGuide.pdf)	Version 6.9.1
SolarWinds Orion Platform 2019.2 Administrator Guide (OrionPlatform20192AdministratorGuide.pdf)	Version 2019.2

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 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.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced all developer tests, as well as additional test cases designed by the evaluator. The evaluator targeted the addition test cases to increase the percentage of TSFI, subsystem and SFR coverage of the developer and increased the coverage for all three dimensions.

2.6.2 Independent penetration testing

The evaluator performed public domain search relating to both the TOE and third party component integrated in the TOE. In addition the evaluator performed an independent vulnerability as 'area of concerns' analysis as follows:

- Analysis of the security architecture of the TOE.
- The SFRs defined in *[ST]* were analysed and for each, a deep understanding of the SFR was gained based on all the evidence provided for ADV.

The total test effort expended by the evaluators was 45 days. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[ST]*. Some testing was performed on an earlier revision of the TOE. The assurance gained from testing on an earlier revision has been assessed to be valid for the final TOE version, because the changes introduced were minimal and did not have an impact on the TSF.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Re-Used Evaluation Results

There is no re-use of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number SolarWinds Orion Suite for Federal Government V4.1. This is further enumerated by the component versions detailed in "Identification of Target of Evaluation", section 2.1 above.

2.9 Results of the Evaluation

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 Orion Suite for Federal Government V4.1, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 2 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. There are no particular obligations or recommendations for the user apart from following the user guidance, and

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

in particular the SolarWinds® Orion® Suite for Federal Government Version 4.1 Common Criteria Supplement.

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.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

3 Security Target

The SolarWinds ORION® Software Security Target Version 2.4, 7 June 2021 *[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:

EOC	Enterprise Operations Console
DBMS	DataBase Management System
IIS	Internet Information Services
IPAM	IP Address Manager
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
LA	Log Analyzer
NCM	Network Configuration Manager
NPM	Network Performance Monitor
NSCIB	Netherlands Scheme for Certification in the area of IT Security
NTA	NetFlow Traffic Analyzer
SAM	Server & Application Monitor
SCM	Server Configuration Monitor
SRM	Storage Resource Monitor
TOE	Target of Evaluation
UDT	User Device Tracker
VMAN	Virtualization Manager
VNQM	VoIP & Network Quality Manager
WPM	Web Performance Monitor

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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 Orion Suite for Federal Government Evaluation Technical Report From UL, serial no. UL12780003/ETR, v2.2, 02 August 2021
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	SolarWinds ORION® Software Security Target Version 2.4, 7 June 2021

(This is the end of this report.)

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.