Certification Report

SolarWinds® Orion® Suite for Federal Government V1.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-286-CR
Version:	1.0
Date:	1 October 2014
Pagination:	i to iii, 1 to 10

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is EWA-Canada.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 1 October 2014, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademarks or registered trademarks:

- SolarWinds and Orion are registered trademarks of SolarWinds Worldwide, LLC.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

SolarWinds® Orion® Suite for Federal Government V1.0 (hereafter referred to as Orion Software), from SolarWinds Worldwide, LLC, is the Target of Evaluation. The results of this evaluation demonstrate that Orion Software meets the requirements of Evaluation Assurance Level (EAL) 2 for the evaluated security functionality.

Orion Software 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 is deployed.

The Orion suite consists of the following network, application, system, and storage monitoring and management components:

- Network Performance Monitor (NPM) 10.6,
- Server & Application Monitor (SAM) 6.0,
- Network Configuration Manager (NCM) 7.2,
- NetFlow Traffic Analyzer (NTA) 3.11,
- IP Address Manager (IPAM) 4.0,
- Voice & Network Quality Manager (VNQM) 4.1,
- User Device Tracker (UDT) 3.0.1,
- Web Performance Monitor (WPM) 2.0.1,
- Enterprise Operations Console (EOC) 1.4.1,
- Failover Engine (FoE) 6.7.0.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 22 August 2014 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Orion Software, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

Communications Security Establishment, as the CCS Certification Body, declares that the Orion Software evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2 evaluation is SolarWinds® Orion® Suite for Federal Government V1.0 (hereafter referred to as Orion Software), from SolarWinds Worldwide, LLC.

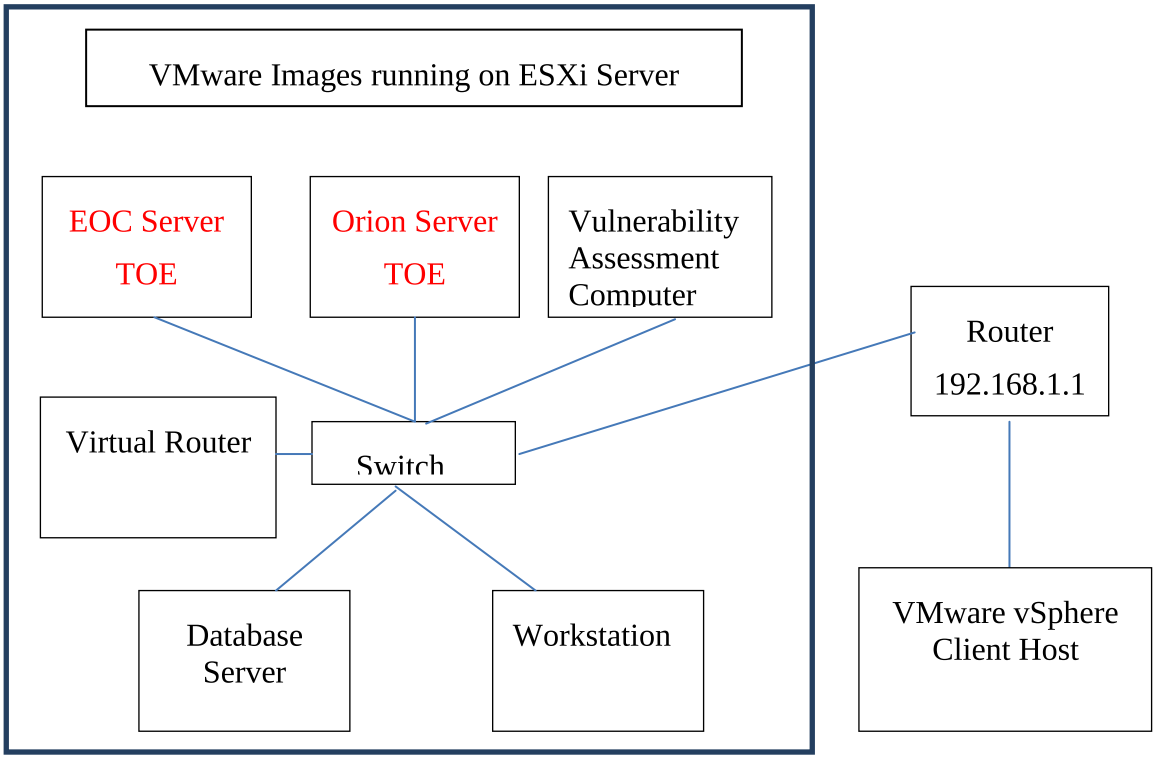
2 TOE Description

Orion Software 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 is deployed.

The Orion suite consists of the following network, application, system, and storage monitoring and management components:

- Network Performance Monitor (NPM) 10.6,
- Server & Application Monitor (SAM) 6.0,
- Network Configuration Manager (NCM) 7.2,
- NetFlow Traffic Analyzer (NTA) 3.11,
- IP Address Manager (IPAM) 4.0,
- Voice & Network Quality Manager (VNQM) 4.1,
- User Device Tracker (UDT) 3.0.1,
- Web Performance Monitor (WPM) 2.0.1,
- Enterprise Operations Console (EOC) 1.4.1,
- Failover Engine (FoE) 6.7.0.

A diagram of the Orion Software architecture is as follows:


VMware Images running on ESXi Server
EOC Server TOE
Orion Server TOE
Vulnerability Assessment Computer
Router
192.168.1.1
Virtual Router
Switch
Database Server
Workstation
VMware vSphere Client Host

3 Security Policy

Orion Software implements a role-based access control policy to control administrative access to the system. In addition, Orion Software implements policies pertaining to the following security functional classes:

- *Security Audit;*
- *Identification and Authentication;*
- *Security Management;*

4 Security Target

The ST associated with this Certification Report is identified below:

SolarWinds® Orion® Software Security Target version 1.9, August 19, 2014

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4,* for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

Orion Software is:

a) EAL 2 conformant, with all security assurance requirements listed for EAL 2.

b) Common Criteria Part 2 extended; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:

- FNM_MDC – Monitor Data Collection;
- FNM_ANL – Monitor Analysis;
- FNM_RCT – Management React;
- FNM_RDR – Restricted Data Review; and
- FNM_STG – Monitor Data Storage.

c) Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3.

6 Assumptions and Clarification of Scope

Consumers of Orion Software should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- Administrators are non-hostile and will follow and abide by the instructions provided by the administrator documentation when using the TOE. Administration is competent and on-going; and

- The Administrator will install and configure the TOE according to the administrator guidance.

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE has access to all the IT System data it needs to perform its functions;

- The TOE is appropriately scalable to the IT Systems the TOE monitors;

- The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation*;* and

- There will be a network that supports communication between distributed components of the TOE. This network functions properly.

7 Evaluated Configuration

The evaluated configuration for Orion Software is a suite of products which include the following:

- One instance of the Orion Enterprise Operations Console (EOC) V1.4.1, installed on a dedicated Windows server.
- One or more instances of the Orion Server, each installed on a dedicated Windows server. Each Orion Server has the following installed:
  a. Network Performance Monitor (NPM) V10.6.0,
  b. Orion Server & Application Monitor (SAM) V6.0.0,
  c. Orion Network Configuration Manager (NCM) V7.2.0,
  d. Orion Netflow Traffic Analyzer (NTA) V3.11.0,
  e. Orion IP Address Manager (IPAM) V4.0.0,
  f. Orion User Device Tracker (UDT) V3.0.1,
  g. Orion Web Performance Monitor (WPM) V2.0.1 and
  h. Orion VoIP & Network Quality Manager (VNQM) V4.1.0
  i. Orion Failover Engine (FoE) V6.7.0 is installed, therefore the Orion Servers must be installed in redundant pairs.

The publications entitled:

- SolarWinds ORION® Suite for Federal Government Common Criteria Supplement, 1.2, 29 July 2014;
- SolarWinds ORION® Common Components Administrator Guide, Version 2013.1.1, 9 September 2013;
- SolarWinds Enterprise Operations Console Administrator Guide, Version 1.4, 21 May 2013;
- SolarWinds NetFlow Traffic Analyzer Administrator Guide, 3.11.0, 1 July 2013;
- SolarWinds IP Address Manager Administrator Guide, Version 4.0, 28 May 2014;
- SolarWinds ORION® Network Performance Monitor Administrator Guide, Version 10.6, 10 September 2013;
- SolarWinds ORION® VoIP and Network Quality Manager Administrator Guide, Version 4.1, 27 August 2013;
- SolarWinds Web Performance Monitor Administrator Guide, 9.9.2013, 9 September 2013;
- SolarWinds® Server and Application Monitor Administrator Guide, Version 6.0, 12 September 2013; and
- SolarWinds® User Device Tracker Administrator Guide, Version 3.0, 23 March 2013.

describe the procedures necessary to install and operate Orion Software in its evaluated configuration.

8 Documentation

In addition to the documents identified in section 7, the following additional SolarWinds® Worldwide, LLC. documents are provided to the consumer:

- SolarWinds® Orion® Network Performance Monitor Quick Start Guide;
- SolarWinds® Technical Reference SolarWinds Orion Web-Based Reports;
- SolarWinds® Network Configuration Manager Administrator Guide;
- SolarWinds® Orion® Network Configuration Manager QuickStart Guide;
- SolarWinds® Failover Engine v6.7 Administrator Guide;
- SolarWinds® Technical Reference Orion® Failover Installation Walkthrough; and
- SolarWinds® Technical Reference Preparing an Orion® Failover Engine Installation.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Orion Software, including the following areas:

Development: The evaluators analyzed the Orion Software functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Orion Software security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Orion Software preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the Orion Software configuration management system and associated documentation was performed. The evaluators found that the Orion Software configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Orion Software during distribution to the consumer.

All these evaluation activities resulted in **PASS** verdicts.

10 ITS Product Testing

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

10.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[1].

The evaluators analyzed the developer’s test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer’s test documentation and the functional specification was complete.

10.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration as identified in the Security Target;

c. Audit: The objective of this test goal is to show audit records are protected, that Logins and Logouts are recorded, as well as Node management changes;

d. Identification and Authentication: The objective of this test goal is to confirm that authentication is required and to confirm that Web console attributes are specific to an individual; and

e. Reports: The objective of this test goal is to demonstrate that users have access to reports and that their access can be managed.

10.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities;

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

b. Information Leakage Verification: The objective of this test goal is to show that traffic between the EOC Server, Orion Server and Database Server is protected;

c. Concurrent User Login: The objective of this test goal is to verify that concurrent administrator logins do not compromise the system;

d. Power Failure: The objective of this test goal is to simulate a power failure situation and verify that the TOE starts up in a proper manner; and

e. Data Misuse: The objective of this test case is to enter invalid data in the Orion Web console field and verify that proper error messages are returned.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

10.4 Conduct of Testing

Orion Software was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test Facility. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that Orion Software behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a EAL 2 level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Evaluator Comments, Observations and Recommendations

The TOE must be installed in accordance with the SolarWinds Orion® Suite for Federal Government Common Criteria Supplement which states which versions of the individual components are required. The supplement also contains detailed configuration settings that must be followed. It is important to ensure that automatic updates are turned off since installing updates would update the product to a version that has not been evaluated.

13 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
EOC	Enterprise Operations Console
FoE	Failover Engine
IPAM	IP Address Manager
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NCM	Network Configuration Manager
NPM	Network Performance Monitor
NTA	Network Traffic Analyzer
PALCAN	Program for the Accreditation of Laboratories - Canada
SAM	Server & Application Monitor
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
UDT	User Device Tracker
VNQM	VOIP and Network Quality Manager
WPM	Web Performance Monitor

14 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. SolarWinds® Orion® Software Security Target version 1.9, August 19, 2014

e. Evaluation Technical Report for SolarWinds Orion Suite for federal Government v1.0, version 1.1, 22 August 2014.