Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

SentinelOne Singularity Complete Version S

19 December 2022

569-LSS

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (a branch of CSE). 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 Canadian Common Criteria Program, and the conclusions of the testing laboratory 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 Canadian Centre for Cyber Security, 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 Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your organization has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Canadian Centre for Cyber Security
Contact Centre and Information Services
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

OVERVIEW

The Canadian Common Criteria Program provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Testing Laboratory (CCTL) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCTL is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the 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, 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 CCTL.

The certification report, certificate of product evaluation and security target are posted to the Common Criteria portal (the official website of the International Common Criteria Program).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

SentinelOne Singularity Complete Version S (hereafter referred to as the Target of Evaluation, or TOE), from **SentinelOne, Inc.** , was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Section 1.1 for the evaluated security functionality.

Lightship Security is the CCTL that conducted the evaluation. This evaluation was completed on **19 December 2022** and was carried out in accordance with the rules of the Canadian Common Criteria Program.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for the TOE, 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.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list (CPL) for the Canadian Common Criteria Program and the Common Criteria portal (the official website of the International Common Criteria Program).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	SentinelOne Singularity Complete Version S
Developer	SentinelOne, Inc.

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

The TOE claims the following conformance:

EAL 2+ (ALC_FLR.2)

1.2 TOE DESCRIPTION

The TOE is an endpoint security platform that provides a single integrated management server and agent to efficiently operate and manage multiple endpoint security solutions. Using advanced Artificial Intelligence (AI), the TOE provides Malware detection and mitigation and external device discovery and control.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

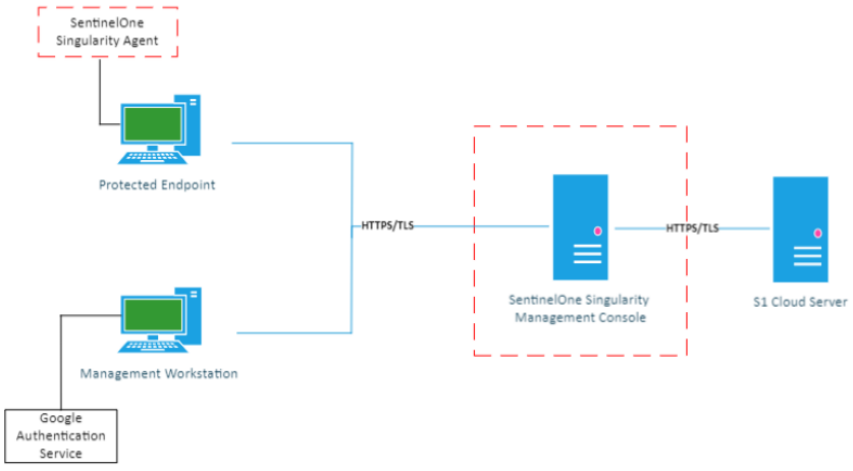

Figure 1: TOE Architecture

2 SECURITY POLICY

The TOE implements and enforces policies pertaining to the following security functionality:

- Secure Management
- Security Dashboard
- Malware Detection & Response
- Protected Communications
- Threat Detection & Response
- External Device Control

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

Consumers of the TOE 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.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- The authentication service in the IT environment will provide two-factor authentication codes for administrators
- The S1 Cloud Server in the IT environment will provide malware analysis services for TOE submitted artifacts
- TOE components are protected from unauthorized physical access
- The IT environment will provide a reliable time source

3.2 CLARIFICATION OF SCOPE

The following functions are outside of the logical TOE scope (and have not been evaluated):

- Firewall Control
- Agent Proxying
- Binary Vault
- Singularity Marketplace
- Cloud (SaaS) Deployment
- Use of Active Directory, LDAP, and SSO authentication
- Remote Shell

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

<table>
<tr><td>TOE Software/Firmware</td><td colspan="4">

Singularity Complete Management Console (Version S, Build #30)
Linux Sentinel Agent 22.1 GA (Build 22.1.2.7)
Windows Sentinel Agent 21.7.5 SP2 (Build 21.7.5.1080)
macOS Sentinel Agent 21.12.2 GA (Build 21.12.2.6003)

</td></tr>
<tr><td rowspan="2">Environmental Support</td><td>Management Console (GPC)

Ubuntu 18.04
CPU: 4 Cores
Memory: 8GB
IOPS: 1K
Disk Space: 500GB

</td><td>Windows Agent (GPC)

Windows 10, Windows Server 2019, or Windows Server 2012R2
1 GHz CPU
1 GB of RAM
2 GB free disk space

</td><td>Linux Agent (GPC)

RHEL 8.3, Ubuntu 20.04, Amazon Linux 2 (Kernel version 4.14), or SLES 15.4.12.14-150.58-default
2 GHz Dual-core CPU
4 GB of RAM
25 GB free disk space

</td><td>macOS agent(GPC)

macOS 11.6
1 GHz CPU
1 GB of RAM
2 GB free disk space

</td></tr>
<tr><td colspan="4">With the following components in the Environment.

S1 Cloud Server
Google Authentication Service

</td></tr>
</table>

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a) SentinelOne Singularity Complete Common Criteria Guide, 8 December 2022, v1.4
b) SentinelOne Singularity Online Help (HTML that is delivered with the TOE and accessed via the management console).

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE 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.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

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

6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent tests, and performing a vulnerability analysis.

6.1 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 Evaluation Test Report (ETR). The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT TESTING

During this evaluation, the evaluator developed independent functional & penetration 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. The following testing activities were performed:

a. Repeat of Developer's Tests: The evaluator repeated a subset of the developer's tests
b. Interoperability Testing: The evaluator verified interoperability between the TOE and a FIPS-validated implementation.
c. Testing of X509 verification (TLS 1.3): The evaluator verified the use of authentication algorithms in TLS 1.3 cipher suites and certificate verification of agents against the TOE UI.

6.3.1 INDEPENDENT TESTING RESULTS

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

6.4 VULNERABILITY ANALYSIS

The vulnerability analysis focused on 4 flaw hypotheses.

- Public Vulnerability based (Type 1)
- Technical community sources (Type 2)
- Evaluation team generated (Type 3)
- Tool Generated (Type 4)

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases and technical community sources (Type 1 & 2). Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities (Type 4). Based upon this review, the evaluators formulated flaw hypotheses (Type 3), which they used in their vulnerability analysis.

Type 1 & 2 searches were conducted on **4 October 2022** and included the following search terms:

Singularity	Sentinel agent	Nginx 1.20
OpenSSL 1.1.1n	OpenSSL 1.1.1j	Docker 20.10.7
Ansible 2.8.1	PostgreSQL 11.13	

Vulnerability searches were conducted using the following sources:

NVD National Vulnerability Database (https://nvd.nist.gov/vuln/search)	CISA Known Exploited Vulnerabilities Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)
Common Vulnerabilities and Exposures (CVE) (http://cve.mitre.org/)	US-CERT (http://www.kb.cert.org/vuls/)
Google (http://www.google.com/)	

6.4.1 VULNERABILITY ANALYSIS RESULTS

The vulnerability analysis did not uncover any security relevant residual exploitable vulnerabilities in the intended operating environment.

7 RESULTS OF THE EVALUATION

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security. This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

The evaluator recommends the TOE as a high-quality endpoint security platform for threat management and response. The TOE implements the security features claimed in a clear and consistent manner with a clear goal of constant upgrades.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCTL	Common Criteria Testing Laboratory
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GPC	General Purpose Computer
IT	Information Technology
ITS	Information Technology Security
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Security Target SentinelOne Singularity Complete Version S, 8 December 2022, v1.7
Evaluation Technical Report SentinelOne Singularity Complete Version S, 19 December 2022, v0.8