Communications Security Establishment Centre de la sécurité des télécommunications

COMMON CRITERIA CERTIFICATION REPORT

Tripwire IP360 Version 9.0.1

4 October 2018

383-4-446

v1.0

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

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 Scheme – 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. 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 CC Scheme, 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.

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

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

OVERVIEW

The Canadian Common Criteria Scheme 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 Certification Body, which is managed by the Communications Security Establishment.

A CCEF 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 17025:2005, 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, 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.

The certification report, certificate of product evaluation and security target are posted to the Certified Products list (CPL) for the Canadian CC Scheme and to the Common Criteria portal (the official website of the International Common Criteria Project).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Tripwire IP360 Version 9.0.1 (hereafter referred to as the Target of Evaluation, or TOE), from Tripwire, 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 TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed 4 October 2018 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for 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.

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

1 IDENTIFICATION OF TARGET OF EVALUATION

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

Table 1 TOE Identification

TOE Name and Version	Tripwire IP360 Version 9.0.1
Developer	Tripwire, Inc.
Conformance Claim	EAL 2 + ALC_FLR.2

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.

1.2 TOE DESCRIPTION

The TOE is a vulnerability and risk management solution that identifies network vulnerabilities, enabling enterprises to protect digital assets from attack. IP360 provides discovery and profiling of network assets, as well as vulnerability scoring and prioritization to identify high risks. It provides a structured approach to detecting, identifying, understanding, and responding to network vulnerabilities.

Tripwire IP360 can be administered remotely or locally, through multiple administrative interfaces, including a command line interface (CLI), a web interface, and two application programming interfaces (APIs).

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

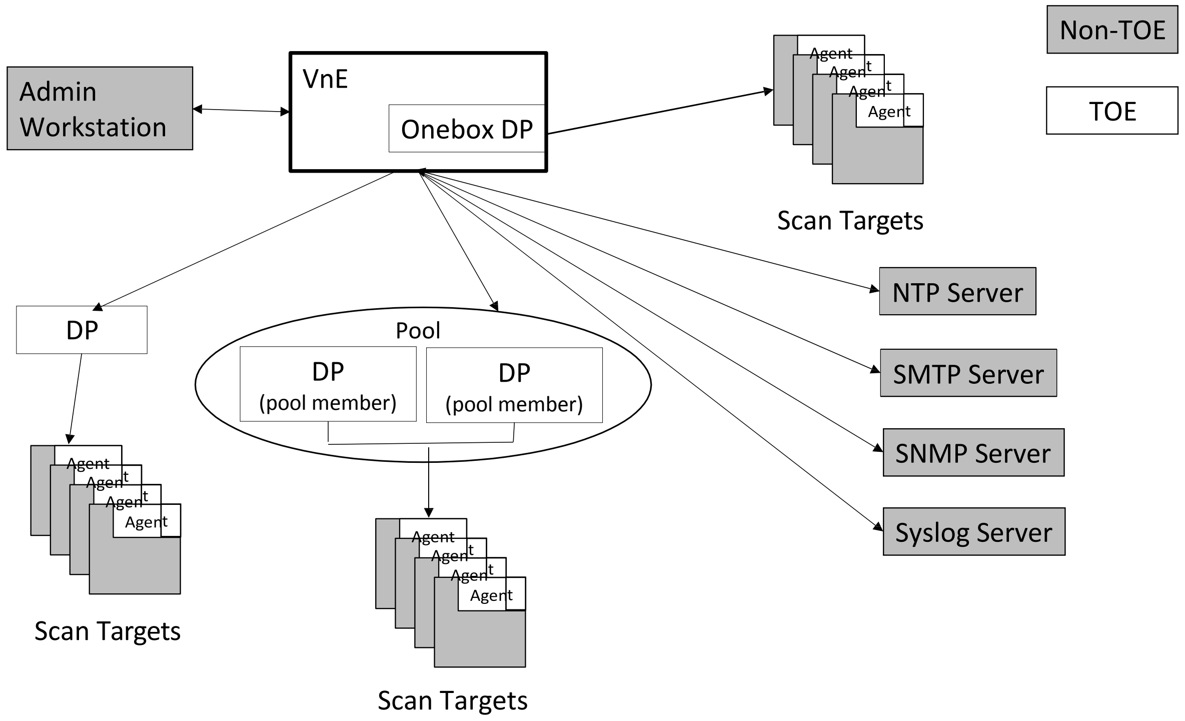

Figure 1 TOE Architecture

2 SECURITY POLICY

The TOE implements policies pertaining to the following security functional classes:

- Security Audit;
- Cryptographic Support;
- Identification and Authentication;
- Security Management;
- Protection of the TSF;
- TOE Access;
- Trusted Path/Channels; and
- Vulnerability Detection System (VDS).

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

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic modules were evaluated by the CMVP and used by the TOE:

Table 2 Cryptographic Module(s)

Cryptographic Module	Certificate Number
OpenSSL FIPS Object Module SE v2.0.16	2398

3 ASSUMPTIONS AND CLARIFICATIONS 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 TOE has access to all of the host system data it needs to perform its functions;
- The TOE is appropriately scalable to the network of host systems the TOE monitors;
- The TOE will be managed in a manner that allows it to appropriately address changes in the host systems the TOE monitors;
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification;
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access; and
- When configured to use a remote time source, the IT environment shall include a trusted source for the system time.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

- The TOE is provided in two configurations, physical hardware appliances or supported virtual platforms. In both cases Tripwire IP360, Version 9.0.1 using Axon Agent version 3.7.0 (VnE build 9.0.1-20180731163509; DP build 9.0.1-20180731141911) is installed on the platform.
- The TOE includes the following physical hardware appliances:
    - DP 6000P
    - VnE 1700
    - VnE 4700
    - VnE 5700
- The TOE includes the following virtual/cloud images:
    - DP EV
    - VnE EV

    The following virtual cloud platforms are in the operating environment for this evaluation:

        - Amazon EC2
        - Microsoft Azure

    The following virtual platforms are in the operating environment for this evaluation:

        - Microsoft Hyper-V 2012 R2
        - VirtualBox 5.X
        - VMware ESXi 6.0, 6.5
        - VMware Fusion 10
        - VMware Workstation 14
- The TOE also includes IP360 Agents which can be installed on the following operating systems in the operating environment:
    - RedHat Enterprise Linux version 7.3 and 7.4 64-bit;
    - Ubuntu 14.0.4 64-bit; and
    - Windows Server 2008, 2008R2, 2012, 2012 R2 64-bit.

4.1 DOCUMENTATION

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

a. Tripwire IP360 9.0.1 Default UI Administrator’s Guide, 8 May 2018;
b. Tripwire IP360 9.0.1 Legacy UI Administrator’s Guide, 30 May 2018;
c. Tripwire IP360 9.0.1 API Guide, 8 May 2018;

d. Tripwire VnE Manager 1700, 4700, 5700 & Ev Quickstart Guide, 8 May 2018;
e. Tripwire IP360 Device Profiler 5000 5050, 6000P & Ev User Guide, 8 May 2018;
f. Tripwire Device Profiler Command Line Interface Guide, 9 May 2018;
g. Tripwire VnE CLI Guide, 8 May 2018;
h. Tripwire IP360 9.0 Agent Based Vulnerability Management Installation and Configuration Guide, 15 May 2018;
i. Tripwire IP360 9.0.1 Agent Based Vulnerability Management Getting Started Guide, 15 May 2018;
j. Tripwire IP360 9.0.1 Release Notes TW 1167-07, 2018; and
k. Tripwire IP360 v9.0.1 Supplemental Common Criteria GuidanceV0.9, 18 September 2018.

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 (SFRs). 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 of 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 functional tests, and performing penetration tests.

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 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 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. The following testing activities were performed:

a. Repeat of Developer's Tests: The evaluator repeated a subset of the developers tests;

b. SSH Supported Data Integrity Algorithm: The objective of this test goal is to confirm that the Device Profiler and VnE Manager accept SSH connections;

c. Protection of Remote Log Server Communications: The objective of this test goal is to confirm that communication between remote syslog server and TOE are encrypted using TLS; and

d. Core Functionality – Vulnerability Scanning: The objective of this test case is to confirm that the core functionality of the TOE is as claimed by comparing a third party scan to the TOE scan.

6.3.1 FUNCTIONAL TEST RESULTS

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

6.4 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 such as Heartbleed, Shellshock, FREAK, POODLE, and GHOST;

b. Information Leakage Verification: The objective of this test goal is to monitor for leakage during start up and shutdown;

c. Web Server Directory Scan: The objective of this test case is to direct a brute force attack on the VnE, looking for hidden web pages available to an unauthenticated user;

d. Weak Data Integrity Algorithm: The objective of this test goal is to verify that the TOE will reject any SSH connection request made with an algorithm not claimed in Security Target; and

e. Misuse: The objective of this test case is to verify the fault tolerance and high availability features.

6.4.1 PENETRATION TEST RESULTS

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

7 RESULTS OF THE EVALUATION

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.

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 5. These evaluation results apply only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

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.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CPL	Certified Products List
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
PP	Protection Profile
SFR	Security Functional Requirement
SSH	Secure Socket Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TLS	Transport Layer Security protocol

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.
Tripwire IP360 Version 9.0.1 Security Target, 10 August 2018, version 0.10
Evaluation Technical Report Tripwire IP360 version 9.0.1, 4 October 2018, version 1.1