National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report

Trustwave AppDetectivePRO v10.2

Report Number: **CCEVS-VR-VID11306-2023**

Dated: **09/20/2023**

Version: **1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Sheldon Durrant

Linda Morrison

The MITRE Corporation

Anne Gugel

Robert Wojcik

Johns Hopkins University - Applied Physics Lab

Common Criteria Testing Laboratory

Shehan Dissanayake

Varsha Shetye

Shivani Birwadkar

Acumen Security, LLC

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Trustwave AppDetectivePRO v10.2 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in September 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended and meets the assurance requirements defined in the Protection Profile for Application Software, Version 1.4, dated 07 October 2021 [SWAPP].

The Target of Evaluation (TOE) is the Trustwave AppDetective Pro v10.2. The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

The technical information included in the report was obtained from the Trustwave AppDetectivePRO v10.2 Security Target, v1.9, September 20, 2023, and analysis performed by the Validation team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Trustwave AppDetectivePRO v10.2
Protection Profile	Protection Profile for Application Software, Version 1.4, dated 07 October 2021 [SWAPP]
Security Target	Trustwave AppDetectivePRO v10.2 Security Target
Evaluation Technical Report	Evaluation Technical Report for Trustwave AppDetectivePRO v10.2
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Extended
Sponsor	Trustwave Holdings Inc
Developer	Trustwave Holdings Inc
Common Criteria Testing Lab (CCTL)	Acumen Security 2400 Research Blvd, Suite 395, Rockville, MD 20850.
CCEVS Validators	Sheldon Durrant, Linda Morrison, Anne Gugel, Robert Wojcik

3 Assumptions & Clarification of Scope

Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile for Application Software, Version 1.4, 7 October 2021 (ASPP14)

That information has not been reproduced here and the ASPP14 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the ASPP14 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation.

Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the PP_APP_v1.4.
- Apart from the Admin Guide, additional customer documentation for the specific Software Application was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the TOE as evaluated.
- This evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The TOE is AppDetectivePRO v10.2 (also referred to as ADP). ADP is application software executing on a Microsoft Windows 10 platform. ADP performs scanning of databases as configured by authorized users. Authorized administrators configure the list of Windows users that may use the ADP application. Authorized users then configure databases (assets) to be scanned, associate policies applicable to each database, and review the results of the scans.

All interactions of administrators and users with the TOE is via a GUI provided by the ADP application. The TOE performs automated scanning of the configured databases hosted on the same Microsoft Windows 10 instance. The scanning functionality is referred to as the Scan Engine. Configuration information is stored in a backend SQLite (v3.35.5) database. .NET is a required component of the Operational Environment.

4.1 TOE Evaluated Platforms

The TOE was tested on a Windows 10 platform.

4.2 TOE Architecture

The TOE product consists of a Windows .exe application installed on a Windows 10 platform.

4.3 Physical Boundaries

The TOE is application software that resides entirely within the application space of a Microsoft Windows 10 instance.

5 Security Policy

This section summaries the security functionality of the TOE:

1. Cryptographic support
2. User data protection
3. Security management
4. Privacy
5. Protection of the TSF
6. Trusted path/channels

5.1 Cryptographic Support

The TOE does not generate keys, use a DRBG or store credentials.

5.2 User Data Protection

The TOE ensures that all sensitive application data is encrypted and protected. The TOE does not maintain sensitive information repositories and it restricts its access only to network connectivity. The TOE restricts inbound and outbound network communications only to user-initiated network communication for scanning configured databases.

5.3 Security Management

The TOE does not come with any default credentials. The user installing the TOE is automatically configured as an authorized Administrator. Administrators may authorize additional users to execute the ADP application. Authorized users may use the ADP application to manage Assets and Policies and execute scans. Scan results may also be viewed.

5.4 Privacy

The TOE itself does not contain or transmit any PII.

5.5 Protection of the TSF

The TOE employs several mechanisms to ensure that it is secure on the host platform. Only documented platform APIs are used by the TOE. The TOE never allocates memory with both write and execute permission. Evaluated platform functionality is used to verify the TOE version and perform updates.

5.6 Trusted Path/Channels

The TOE does not transmit sensitive data.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Trustwave AppDetectivePRO User Guide, Version 10.2, July 2021

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the proprietary detailed Test Report, Trustwave AppDetectivePRO v10.2, v1.3, September 8, 2023, and is summarized in the evaluation Assurance Activity Report (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

7.2 Evaluation Team Independent Testing

The Evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the ASPP14.

8 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Trustwave AppDetectivePRO v10.2 to be Part 2 extended, and meets the SARs contained in the PP_APP_v1.4..

8.1 Evaluation of Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Trustwave AppDetectivePRO v10.2 that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.2 Evaluation of Development Documentation (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the Evaluation team was justified.

8.3 Evaluation of Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the Evaluation team was justified.

8.4 Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.5 Evaluation of Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the PP_APP_v1.4 and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence was provided by the Evaluation to confirm that the evaluation was conducted in accordance with the requirements of the CEM,, and that the conclusion reached by the Evaluation team was justified.

8.6 Vulnerability Assessment Activity (VAN)

The Evaluation team applied each AVA CEM work unit. The Evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The Evaluation team searched:

- http://nvd.nist.gov/
- http://www.us-cert.gov
- http://www.securityfocus.com/
- https://www.cvedetails.com/

The Evaluation team performed the public domain vulnerability searches on September 8, 2023, using the following key words.

- AppDetectivePRO
- Trustwave
- Microsoft .NET Framework 4.8
- Microsoft SQL Server 2017
- SQLite 3.35.5
- Java SE 8 Java Runtime Environment
- Java Runtime Environment
- Windows Defender Exploit Guard

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.7 Summary of Evaluation Results

The Evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

9 Validator Comments & Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the AppDetectivePRO Version 10.2 User Guide, July 2021. No versions of the TOE software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation.

10 Annexes

Not applicable.

11 Security Target

Trustwave AppDetectivePRO v10.2 Security Target, Version 1.9, September 20, 2023.

12 Glossary

The following definitions are used throughout this document:

Term	Definition
Common Criteria Testing Laboratory (CCTL)	An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
Conformance	The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
Evaluation	The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
Evaluation Evidence	Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
Feature	Part of a product that is either included with the product or can be ordered separately.
Target of Evaluation (TOE)	A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
Validation	The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
Validation Body	A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5, April 2017.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5, April 2017.
4. Protection Profile for Application Software, Version 1.4, 7 October 2021 (ASPP14).
5. Trustwave AppDetectivePRO v10.2 Security Target, Version 1.9, September 20, 2023.
6. Trustwave AppDetectivePRO User Guide, v10.2, July 2021
7. Assurance Activity Report for Trustwave, Version 1.5, September 20, 2023
8. Test Report for Trustwave AppDetectivePRO v10.2, Version 1.3, September 8, 2023.
9. Evaluation Technical Report for Trustwave AppDetectivePRO v10.2, Version 1.5, September 20, 2023.