Assurance Activity Report for
Trustwave AppDetectivePRO v10.2

Trustwave AppDetectivePRO Security Target
Version 1.9

Protection Profile for Application Software, Version 1.4

AAR Version 1.5, September 20, 2023

Evaluated by:

2400 Research Blvd, Suite 395
Rockville, MD 20850

Prepared for:

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
Trustwave Holdings Inc

The Author of the Security Target:
Acumen Security, LLC

The TOE Evaluation was Sponsored by:
Trustwave Holdings Inc

Evaluation Personnel:
Acumen Security, LLC
Shehan Dissanayake
Varsha Shetye
Shivani Birwadkar

Common Criteria Version
Common Criteria Version 3.1 Revision 5

Common Evaluation Methodology Version
CEM Version 3.1 Revision 5

Revision History

VERSION	DATE	CHANGES
1.0	12/06/2023	Initial Release
1.1	21/07/2023	Updates to address NIAP comments
1.2	11/08/2023	Minor updates to address NIAP comments
1.3	08/09/2023	Update to the ST version, minor updates to section 6.18 and 7.4.1
1.4	13/09/2023	Minor update to section 6.18 Pass/Fail explanation
1.5	20/09/2023	Update to ST version

Contents

`

1 TOE Overview

AppDetectivePRO (also referred to as ADP) is application software that 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.

2 Assurance Activities Identification

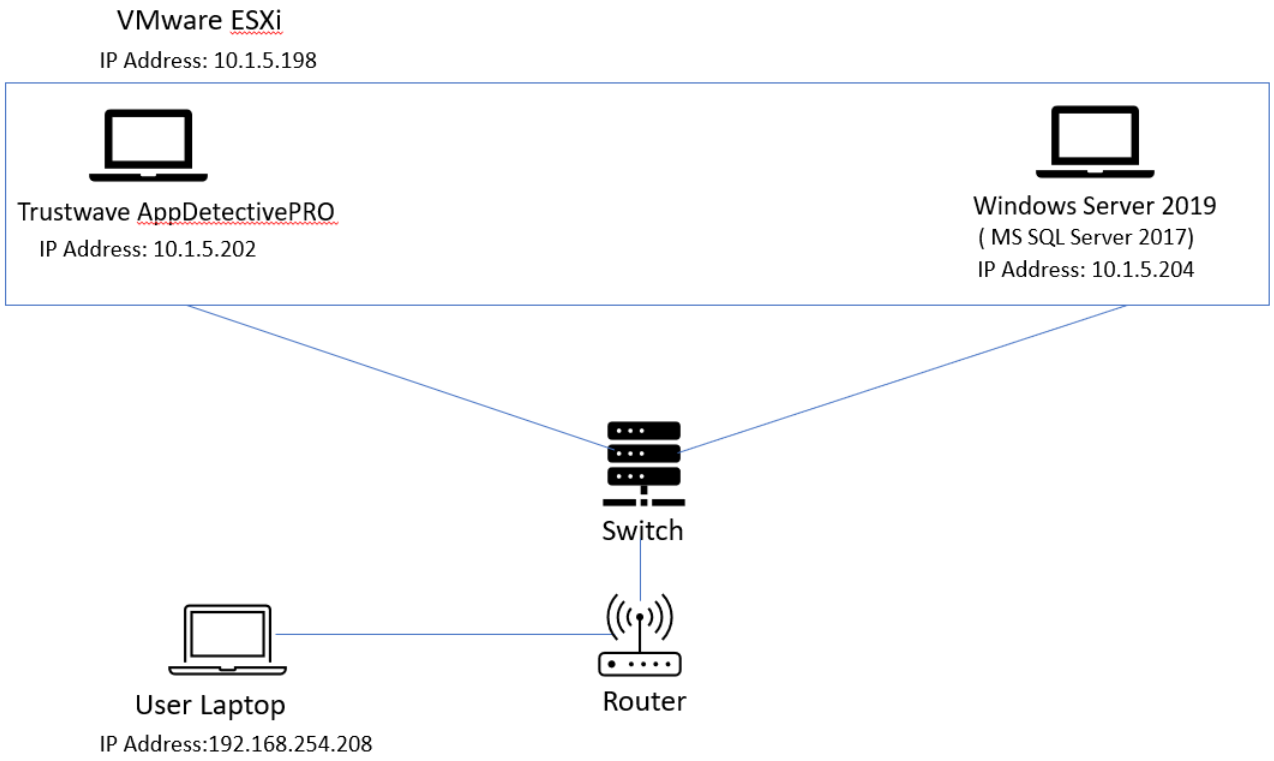
The Assurance Activities contained within this document include all those defined within the PP_APP_v1.4 based upon the core SFRs and those implemented based on selections within the PP.

3 Test Equivalency Justification

The TOE is evaluated on the platform as identified in Section 1. No equivalency argument is needed.

4 Test Bed Descriptions

4.1 Test Bed Diagram



4.2 Test Bed Details

Device Details		System Details		
Role in test environment	**Device Name**	**OS, including version**	**Timing Source**	**Software & Tools, including version**
TOE	Trustwave AppDetectivePRO	Windows 10	Manual	AppDetectivePRO v10.2, SQLite 3.35.5, JRE, .Net 4.8, Wiresharkv3.0.3, Process Monitor tool, Access Check tool v6.14, VMMap tool, Microsoft's BinScope Binary Analyzer tool 2014, Microsoft Network Monitor tool v3.4
Tester's Laptop	Laptop	Windows 10	Manual	Wiresharkv3.0.3
Virtual Machine	Windows Server 2019	Windows Server 2019	Manual	Microsoft SQL Server 2017
VMware ESXi	VMware ESXi 6.7	Windows 10	Manual	Windows 10 Enterprise, Windows Server 2019, Ubuntu Desktop.

4.3 Test Time & Location

All testing was carried at the Acumen Security offices located in 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from December 6, 2021 to July 20, 2023.

The TOE was in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. At the start of each day, the test bed was verified to ensure that it was not compromised. All evaluation documentation was always kept with the evaluator.

5 Detailed Test Cases (TSS and Guidance Activities)

5.1 TSS and Guidance Activities (Cryptographic Support)

5.1.1 FCS_CKM_EXT.1

5.1.1.1 FCS_CKM_EXT.1 TSS 1

Objective	The evaluator shall inspect the application and its developer documentation to determine if the application needs asymmetric key generation services. If not, the evaluator shall verify the **generate no asymmetric cryptographic keys** selection is present in the ST. Otherwise, the evaluation activities shall be performed as stated in the selection-based requirements.
Evaluator Findings	The evaluator examined the SFR section in the Security Target and determined that the "generate no asymmetric cryptographic keys" selection is present in the ST. In addition, the evaluator used the TOE extensively during testing and determined that it does not use any services that would require the generation of asymmetric cryptographic keys. Evaluator also examined the application developer documentation and no evidence to support the use of such services was found. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2 FCS_RBG_EXT.1

5.1.2.1 FCS_RBG_EXT.1 TSS 1

Objective	If use no DRBG functionality is selected, the evaluator shall inspect the application and its developer documentation and verify that the application needs no random bit generation services. If "implement DRBG functionality" is selected, the evaluator shall ensure that additional FCS_RBG_EXT.2 elements are included in the ST. If "invoke platform-provided DRBG functionality" is selected, the evaluator performs the following activities. The evaluator shall examine the TSS to confirm that it identifies all functions (as described by the SFRs included in the ST) that obtain random numbers from the platform RBG. The evaluator shall determine that for each of these functions, the TSS states which platform interface (API) is used to obtain the random numbers. The evaluator shall confirm that each of these interfaces corresponds to the acceptable interfaces listed for each platform below. It should be noted that there is no expectation that the evaluators attempt to confirm that the APIs are being used correctly for the functions identified in the TSS; the activity is to list the used APIs and then do an existence check via decompilation.
Evaluator Findings	The ST claims '*use no DRBG functionality*' for **FCS_RBG_EXT.1**. The evaluator examined all the sections of the developer documentation and inspected the application throughout the testing process to verify that the application needs no random bit generation services. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3 FCS_STO_EXT.1

5.1.3.1 FCS_STO_EXT.1 TSS 1

Objective	The evaluator shall check the TSS to ensure that it lists all persistent credentials (secret keys, PKI private keys, or passwords) needed to meet the requirements in the ST. For each of these items, the evaluator shall confirm that the TSS lists for what purpose it is used, and how it is stored.
Evaluator Findings	Upon investigation, the evaluator found that the TSS states that: ***The TOE does not store any credentials. Credentials used when scanning databases are only saved in memory for use in the immediate scan; they are never saved in non-volatile memory.*** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2 TSS and Guidance Activities (User Data Protection)

5.2.1 FDP_DAR_EXT.1

5.2.1.1 FDP_DAR_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that it describes the sensitive data processed by the application. The evaluator shall then ensure that the [test] activities [in the PP] cover all of the sensitive data identified in the TSS.
Evaluator Findings	The evaluator examined the **FDP_DAR_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes the sensitive data processed by the application. Upon investigation, the evaluator found that the TSS states that: ***The Application temporarily saves the sensitive data such as the credentials of the remote scanning databases in the volatile memory and are destroyed when the application is shut down. The data such as the hostname/IP, port, and protocol information are stored on the local drive.*** The evaluator also examined the section titled **1.2 Typical System Requirements** in the AGD and found that it provides the following clear guidance to the end-users on how to encrypt data-at-rest: ***Caution: It is the recommendation of Trustwave that, to protect data at rest, AppDetectivePRO should be installed on a system drive that has the Windows Bitlocker feature enabled on.*** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.1.2 FDP_DAR_EXT.1 TSS 2

Objective	If **not store any sensitive data** is selected, the evaluator shall inspect the TSS to ensure that it describes how sensitive data cannot be written to non-volatile memory. The evaluator shall also ensure that this is consistent with the filesystem test [in the PP].
Evaluator Findings	This assurance activity is considered not applicable because “not store any sensitive data” is not selected.
Verdict	N/A

5.2.2 FDP_DEC_EXT.1

5.2.2.1 FDP_DEC_EXT.1.1 Guidance 1

Objective	The evaluator shall perform the platform-specific [test] actions [in the PP] and inspect user documentation to determine the application's access to hardware resources. The evaluator shall ensure that this is consistent with the selections indicated.
Evaluator Findings	The ST claims 'the application shall restrict its access to **network connectivity**'. The evaluator examined the section titled **1.2 Typical System Requirements** in the AGD to verify that the stated hardware access is consistent with the SFR selections. Upon investigation, the evaluator found that the AGD states that: ***Networking*** • ***ASAP Update requires access to the internet.*** • ***Scan of asset(s) require network connection access to the asset(s).*** The evaluator also examined the section titled **1.2 Typical System Requirements** in the AGD to verify that the stated hardware access is consistent with the results obtained from the test assurance activities. Upon investigation, the evaluator found that the hardware access information is consistent. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2.2 FDP_DEC_EXT.1.1 Guidance 2

Objective	The evaluator shall review documentation provided by the application developer and for each resource which it accesses, identify the justification as to why access is required.
Evaluator Findings	The ST claims 'the application shall restrict its access to **network connectivity**'. The evaluator examined the section titled **1.2 Typical System Requirements** in the AGD to identify, for each resource which it accesses, the justification as to why access is required. Upon investigation, the evaluator found that the AGD states that: ***Networking*** • ***ASAP Update requires access to the internet.*** • ***Scan of asset(s) require network connection access to the asset(s).*** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2.3 FDP_DEC_EXT.1.2 Guidance 1

Objective	The evaluator shall perform the platform-specific [test] actions [in the PP] and inspect user documentation to determine the application's access to sensitive information repositories. The evaluator shall ensure that this is consistent with the selections indicated.
Evaluator Findings	The ST claims 'the application shall restrict its access to **no sensitive information repositories**'.

	The evaluator examined the AGD and found no information about sensitive information repositories that are being accessed by the TOE or are being restricted. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2.4 FDP_DEC_EXT.1.2 Guidance 2

Objective	The evaluator shall review documentation provided by the application developer and for each sensitive information repository which it accesses, identify the justification as to why access is required.
Evaluator Findings	The evaluator examined the AGD and found no information about sensitive information repositories that are being accessed by the TOE or are being restricted. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

TSS and Guidance Activities (Security Management)

5.2.3 FMT_CFG_EXT.1

5.2.3.1 FMT_CFG_EXT.1.1 TSS 1

Objective	The evaluator shall check the TSS to determine if the application requires any type of credentials and if the application installs with default credentials.
Evaluator Findings	The evaluator examined the **FMT_CFG_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to determine if the application requires any type of credentials and if the application installs with default credentials. Upon investigation, the evaluator found that the TSS states that: ***The TOE does not authenticate users. The TOE does maintain an internal list of Windows users that are authorized to use the ADP application. When the application is invoked, the user id of the user is checked against the list of authorized users. If the user is not authorized, an error message is displayed and then the application closes.*** ***When the TOE is installed, the user id of the person performing the installation is automatically configured as the only authorized Administrator. That Administrator may execute the application and add other user ids to the authorized user list.*** ***By default, the TOE binaries and data are configured with file permissions which protect the application binaries and data files from modification by normal unprivileged users.*** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.4 FMT_MEC_EXT.1

5.2.4.1 FMT_MEC_EXT.1 TSS 1

Objective	The evaluator shall review the TSS to identify the application's configuration options (e.g. settings) and determine whether these are stored and set using the mechanisms supported by the platform or implemented by the application in accordance with the PP-Module for File Encryption. At a minimum the TSS shall list settings related to any SFRs and any settings that are mandated in the operational guidance in response to an SFR.

Evaluator Findings	The evaluator examined the **FMT_MEC_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies the application's configuration options (e.g. settings) and determine whether these are stored and set using the mechanisms supported by the platform or implemented by the application in accordance with the PP-Module for File Encryption. Upon investigation, the evaluator found that the TSS states that: ***ADP stores configuration data under the ProgramData directory.*** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.4.2 FMT_MEC_EXT.1 TSS 2

Objective	**Conditional:** If "implement functionality to encrypt and store configuration options as defined by FDP_PRT_EXT.1 in the PP-Module for File Encryption" is selected, the evaluator shall ensure that the TSS identifies those options, as well as indicates where the encrypted representation of these options is stored.
Evaluator Findings	The evaluator examined the SFR in the Security Target and determined that implement functionality to encrypt and store configuration options as defined by FDP_PRT_EXT.1 in the PP-Module for File Encryption is not selected. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.5 FMT_SMF.1

5.2.5.1 FMT_SMF.1 Guidance 1

Objective	The evaluator shall verify that every management function mandated by the PP is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function.
Evaluator Findings	The evaluator examined the section titled **Understanding the AppDetectivePRO User Interface** in the AGD to verify that every management function mandated by the PP is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function. Upon investigation, the evaluator found that the AGD states that: The user interface allows you to see different sections at a time. It has three main areas where you can perform different tasks: Sessions, Policies, and System Settings. • Sessions: manage assets and perform all your different scans, review results, and run scan reports • Policies: view how the built-in policies are configured and create any custom policies • System Settings: configure users of the product, run ASAP Updates, and change other settings When working in Sessions and Policies, you see data laid out in a grid control format. At any time, you can choose to sort and group by different attributes of the data you are viewing by dragging and dropping the attributes from the top row. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.3 TSS and Guidance Activities (Privacy)

5.3.1 FPR_ANO_EXT.1

5.3.1.1 FPR_ANO_EXT.1 TSS 1

Objective	The evaluator shall inspect the TSS documentation to identify functionality in the application where PII can be transmitted.
Evaluator Findings	The evaluator examined the **FPR_ANO_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies functionality in the application where PII can be transmitted. Upon investigation, the evaluator found that the TSS states that: The TOE does not transmit PII over the network. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4 TSS and Guidance Activities (Protection of the TSF)

5.4.1 FPT_AEX_EXT.1

5.4.1.1 FPT_AEX_EXT.1.1 TSS 1

Objective	The evaluator shall ensure that the TSS describes the compiler flags used to enable ASLR when the application is compiled.
Evaluator Findings	The evaluator examined the **FPT_AEX_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes the compiler flags used to enable ASLR when the application is compiled. Upon investigation, the evaluator found that the TSS states that: No components of the TOE are compiled with the flags required to disable ASLR. Therefore, no memory is mapped to an explicit address. The TOE does not allocate any memory region with both write and execute permissions. The TOE is compatible with Windows Defender Exploit Guard. The TOE does not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so. By default, the TOE writes logs to subdirectories of the install directory, but no executables are present in those subdirectories. All ADP components are written with the .NET framework, which automatically has stack-based overflow protections enabled. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.2 FPT_API_EXT.1

5.4.2.1 FPT_API_EXT.1TSS 1

Objective	The evaluator shall verify that the TSS lists the platform APIs used in the application.

Evaluator Findings	The evaluator examined the **FPT_API_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS lists the platform APIs used in the application. Upon investigation, the evaluator found that the TSS states that: The TOE uses the following platform APIs: • Microsoft.Expression.Interactions.dll • Microsoft.SqlServer.Types.dll • Microsoft,dynamic.dll • Microsoft.scripting.dll The Microsoft.dynamic.dll and Microsoft.scripting.dll are Microsoft-produced libraries that are used in the.NET 4 stack to facilitate Dynamic Language Runtime (DLR) functionality. This functionality is in the scripting.dll which in turn needs the Microsoft.dynamic.dll. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.3 FPT_IDV_EXT.1

5.4.3.1 FPT_IDV_EXT.1 TSS 1

Objective	If "other version information" is selected the evaluator shall verify that the TSS contains an explaination of the versioning methodology.
Evaluator Findings	The evaluator examined the **FPT_IDV_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS contains an explanation of the versioning methodology. Upon investigation, the evaluator found that the TSS states that: The TOE uses “Major.Minor.Incremental” versioning. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.4 FPT_TUD_EXT.1

5.4.4.1 FPT_TUD_EXT.1.1 Guidance 1

Objective	The evaluator shall check to ensure the guidance includes a description of how updates are performed.
Evaluator Findings	The evaluator examined the section titled **System Settings** in the AGD to verify that it includes a description of how updates are performed. Upon investigation, the evaluator found that the AGD states that: System Settings allow you to configure users of the product, run ASAP Updates, see the version of the product, change log file trace settings, and view licensing information. The following sections are available: ASAP Updater allows you to stay up-to-date with the latest product version and SHATTER Knowledgebase. When logged in as an administrator, you can launch the update to download the latest available versions. You can also configure a proxy if needed. The “disable ASAP

	Updates" checkbox will disable this functionality ensuring the AppDetectivePRO installation will not change (updates may drop support for older database versions). Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.4.2 FPT_TUD_EXT.1.2 Guidance 1

Objective	The evaluator shall verify guidance includes a description of how to query the current version of the application.
Evaluator Findings	The evaluator examined the section titled **System Settings** in the AGD to verify that it includes a description of how to query the current version of the application. Upon investigation, the evaluator found that the AGD states that: System Settings allow you to configure users of the product, run ASAP Updates, see the version of the product, change log file trace settings, and view licensing information. The following sections are available: • About: displays the versions of each component of AppDetectivePRO. You may need to provide this information to the Customer Support team if working on an issue. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.4.3 FPT_TUD_EXT.1.4 TSS 1

Objective	The evaluator shall verify that the TSS identifies how updates to the application are signed by an authorized source. The definition of an authorized source must be contained in the TSS. The evaluator shall also ensure that the TSS (or the operational guidance) describes how candidate updates are obtained.
Evaluator Findings	The evaluator examined the **FPT_TUD_EXT.2** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies how updates to the application are signed by an authorized source. Upon investigation, the evaluator found that the TSS states that: TOE updates are distributed as a signed installer (MSI). Update packages are verified by Windows prior to installation. The signing is done with a code signing certificate issued by a trusted Certificate Authority. All updates to ADP are provided through the Fusion customer portal (https://fusion.trustwave.com/) for download. A SHA1 hash is also provided to the customers to validate the files. The evaluator also examined the **FPT_TUD_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS (or the operational guidance) describes how candidate updates are obtained. Upon investigation, the evaluator found that the TSS states that: The platform is used to check for TOE updates. The TOE does not download or modify its own code. The TOE provides the ability to query the currently-executing version. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.4.4 FPT_TUD_EXT.1.5 TSS 1

Objective	The evaluator shall verify that the TSS identifies how the application is distributed. If "with the platform" is selected the evaluated shall perform a clean installation or factory reset to confirm that TOE software is included as part of the platform OS. If "as an additional package" is selected the evaluator shall perform the tests in FPT_TUD_EXT.2.
Evaluator Findings	The evaluator examined the **FPT_TUD_EXT.1** entry and **FPT_TUD_EXT.2** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies how the application is distributed. Upon investigation, the evaluator found that the TSS states that: The application can be downloaded from the downloads section of the Trustwave web platform using the account created by the order fulfillment team of Trustwave ((https://fusion.trustwave.com/). The node-locked license is generated by the order fulfilment team of Trustwave is sent separately via email. A SHA1 hash is also provided to the customers to validate the downloaded files. The TSS also describes how the updates are distributed: TOE updates are distributed as a signed installer (MSI). Update packages are verified by Windows prior to installation. The signing is done with a code signing certificate issued by a trusted Certificate Authority. All updates to ADP are provided through the Fusion customer portal (https://fusion.trustwave.com/) for download. A SHA1 hash is also provided to the customers to validate the files. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.5 FPT_TUD_EXT.2

5.4.5.1 FPT_TUD_EXT.2.3 TSS 1

Objective	The evaluator shall verify that the TSS identifies how the application installation package is signed by an authorized source. The definition of an authorized source must be contained in the TSS.
Evaluator Findings	The evaluator examined the **FPT_TUD_EXT.1** entry and **FPT_TUD_EXT.2** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies how the application installation package is signed by an authorized source. Upon investigation, the evaluator found that the TSS states that: TOE application and the updates are distributed as a signed installer (MSI). Update packages are verified by Windows prior to installation. The signing is done with a code signing certificate issued by a trusted Certificate Authority. A SHA1 hash is also provided to the customers to validate the downloaded files. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5 TSS and Guidance Activities (Trusted Path/Channels)

5.5.1 FTP_DIT_EXT.1

5.5.1.1 FTP_DIT_EXT.1 TSS 1

Objective	For platform-provided functionality, the evaluator shall verify the TSS contains the calls to the platform that TOE is leveraging to invoke the functionality.
Evaluator Findings	Upon investigation, the evaluator found that the TSS states that: The TOE does not transmit sensitive data. Based on these findings, this assurance activity is considered not applicable because "platform-provided functionality" is not selected in the ST.
Verdict	N/A

6 Detailed Test Cases (Test Activities)

6.1 FCS_STO_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	For all credentials for which **the application implements functionality**, the evaluator shall verify credentials are encrypted according to FCS_COP.1/SKC or conditioned according to FCS_CKM.1.1/AK and FCS_CKM.1/PBKDF.
Pass/Fail with Explanation	NA. The ST does not select "**implements functionality".**

6.2 FCS_STO_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	For all credentials for which the application **invokes platform-provided functionality**, the evaluator shall perform the following actions which vary per platform. **Platforms:Android...** The evaluator shall verify that the application uses the Android KeyStore or the Android KeyChain to store certificates. ***Platforms:Microsoft Windows...*** *The evaluator shall verify that all certificates are stored in the Windows Certificate Store. The evaluator shall verify that other credentials, like passwords, are stored in the Windows Credential Manager or stored using the Data Protection API (DPAPI). For Windows Universal Applications, the evaluator shall verify that the application is using the ProtectData class and storing credentials in IsolatedStorage.* **Platforms:Apple iOS...** The evaluator shall verify that all credentials are stored within a Keychain. **Platforms:Linux...** The evaluator shall verify that all keys are stored using Linux keyrings. **Platforms:Oracle Solaris...** The evaluator shall verify that all keys are stored using Solaris Key Management Framework (KMF). **Platforms:Apple macOS...** The evaluator shall verify that all credentials are stored within Keychain.
Pass/Fail with Explanation	NA. The ST does not select "**invokes platform-provided functionality**".

6.3 FDP_DAR_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	Evaluation activities (after the identification of the sensitive data) are to be performed on all sensitive data listed that are not covered by FCS_STO_EXT.1. If "implement functionality to encrypt sensitive data as defined in the PP-Module for File Encryption" or "protect sensitive data in accordance with FCS_STO_EXT.1" is selected, the evaluator shall inventory the filesystem locations where the application may write data. The evaluator shall run the application and attempt to store sensitive data. The evaluator shall then inspect those areas of the filesystem to note where data was stored (if any), and determine whether it has been encrypted. **TD00756 has been applied.**

Test Steps	• Start the application and attempt to store sensitive data. • Note the locations where application writes data. • Verify that locations where data was stored are encrypted.
Expected Test Results	• The locations where application writes data should be encrypted. • Evidence (screenshots) showing locations where data was stored.
Pass/Fail with Explanation	Pass. The data stored in the location of the software's Backend Configuration is encrypted.

6.4 FDP_DAR_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	Evaluation activities (after the identification of the sensitive data) are to be performed on all sensitive data listed that are not covered by FCS_STO_EXT.1. If **leverage platform-provided functionality** is selected, the evaluation activities will be performed as stated in the following requirements, which vary on a per-platform basis. **Platforms:Android...** The evaluator shall inspect the TSS and verify that it describes how files containing sensitive data are stored with the MODE_PRIVATE flag set. ***Platforms:Microsoft Windows...*** *The Windows platform currently does not provide data-at-rest encryption services which depend upon invocation by application developers. The evaluator shall verify that the Operational User Guidance makes the need to activate platform encryption, such as BitLocker or Encrypting File System (EFS), clear to the end user.* **Platforms:Apple iOS...** The evaluator shall inspect the TSS and ensure that it describes how the application uses the Complete Protection, Protected Unless Open, or Protected Until First User Authentication Data Protection Class for each data file stored locally. **Platforms:Linux...** The Linux platform currently does not provide data-at-rest encryption services which depend upon invocation by application developers. The evaluator shall verify that the Operational User Guidance makes the need to activate platform encryption clear to the end user. **Platforms:Oracle Solaris...** The Solaris platform currently does not provide data-at-rest encryption services which depend upon invocation by application developers. The evaluator shall verify that the Operational User Guidance makes the need to activate platform encryption clear to the end user. **Platforms:Apple macOS...** The macOS platform currently does not provide data-at-rest encryption services which depend upon invocation by application developers. The evaluator shall verify that the Operational User Guidance makes the need to activate platform encryption clear to the end user.
Test Steps	• Verify the Operational User Guidance mentions the need to activate platform encryption. • Verify that BitLocker was activated on the system.
Expected Test Results	• The Operational User Guidance should mention the need to activate platform encryption clear to the end user. • Evidence (screenshots) showing that Bitlocker is activated on the system.

Pass/Fail with Explanation	Pass. The entire contents of the file system are encrypted, ensuring that all data including configuration files and metadata written by the TOE are encrypted. It has been verified that the Operational User Guidance makes the need to activate platform encryption clear to the end user.

6.5 FMT_CFG_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	If the application uses any default credentials the evaluator shall run the following tests. **Test 1:** The evaluator shall install and run the application without generating or loading new credentials and verify that only the minimal application functionality required to set new credentials is available.
Pass/Fail with Explanation	NA. The TOE is not installed with default credentials.

6.6 FMT_CFG_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	If the application uses any default credentials the evaluator shall run the following tests. **Test 2:** The evaluator shall attempt to clear all credentials and verify that only the minimal application functionality required to set new credentials is available.
Pass/Fail with Explanation	NA. The TOE is not installed with default credentials.

6.7 FMT_CFG_EXT.1.1 Test #3

Item	Data
Test Assurance Activity	If the application uses any default credentials the evaluator shall run the following tests. **Test 3:** The evaluator shall run the application, establish new credentials and verify that the original default credentials no longer provide access to the application.
Pass/Fail with Explanation	NA. The TOE is not installed with default credentials.

6.8 FMT_CFG_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	The evaluator shall install and run the application. The evaluator shall inspect the filesystem of the platform (to the extent possible) for any files created by the application and ensure that their permissions are adequate to protect them. The method of doing so varies per platform. **Platforms:Android...** The evaluator shall run the command find -L . -perm /002 inside the application's data directories to ensure that all files are not world-writable. The command should not print any files. ***Platforms:Microsoft Windows...*** *The evaluator shall run the SysInternals tools, Process Monitor and Access Check (or tools of equivalent capability, like icacls.exe) for Classic Desktop applications to verify that files written to disk during an application's installation have the correct file permissions, such that a standard user cannot modify the application or its data files. For Windows Universal*

	Applications the evaluator shall consider the requirement met because of the AppContainer sandbox. **Platforms:Apple iOS...** The evaluator shall determine whether the application leverages the appropriate Data Protection Class for each data file stored locally. **Platforms:Linux...** The evaluator shall run the command find -L . -perm /002 inside the application's data directories to ensure that all files are not world-writable. The command should not print any files. **Platforms:Oracle Solaris...** The evaluator shall run the command find . \(-perm -002 \) inside the application's data directories to ensure that all files are not world-writable. The command should not print any files. **Platforms:Apple macOS...** The evaluator shall run the command find . -perm +002 inside the application's data directories to ensure that all files are not world-writable. The command should not print any files.
Test Steps	• Start the TOE application service. • Run the SysInternals tool 'Process Monitor' to monitor the events of the application files and ensure that the application or data files have correct file permissions such that the files cannot be modified by a standard user. • Run the SysInternals tool 'Access Check' to ensure that the application or data files have correct file permissions such that the files cannot be modified by a standard user.
Expected Test Results	• The application and data files should be protected and cannot be modified without authentication. • Evidence (screenshots) showing files written to the disk during the installation of TOE have correct file permissions.
Pass/Fail with Explanation	Pass. It has been verified that the application or data files have correct file permissions such that the files cannot be modified by a standard user.

6.9 FMT_MEC_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	If "**invoke the mechanisms recommended by the platform vendor for storing and setting configuration options**" is chosen, the method of testing varies per platform as follows: **Platforms:Android...** The evaluator shall run the application and make security-related changes to its configuration. The evaluator shall check that at least one XML file at location /data/data/package/shared_prefs/ reflects the changes made to the configuration to verify that the application used SharedPreferences and/or PreferenceActivity classes for storing configuration data, where package is the Java package of the application. ***Platforms:Microsoft Windows...*** *The evaluator shall determine and verify that Windows Universal Applications use either the Windows.Storage namespace, Windows.UI.ApplicationSettings namespace, or the IsolatedStorageSettings namespace for storing application specific settings. For .NET applications, the evaluator shall determine and verify that the application uses one of the locations listed in https://docs.microsoft.com/en-us/dotnet/framework/configure-apps/ for storing application specific settings. For Classic Desktop applications, the evaluator shall run the application while monitoring it with the SysInternals tool ProcMon and make*

	changes to its configuration. The evaluator shall verify that ProcMon logs show corresponding changes to the the Windows Registry or C:\ProgramData\ directory. **Platforms:Apple iOS...** The evaluator shall verify that the app uses the user defaults system or key-value store for storing all settings. **Platforms:Linux...** The evaluator shall run the application while monitoring it with the utility strace. The evaluator shall make security-related changes to its configuration. The evaluator shall verify that strace logs corresponding changes to configuration files that reside in /etc (for system-specific configuration), in the user's home directory (for user-specific configuration), or /var/lib/ (for configurations controlled by UI and not intended to be directly modified by an administrator). **Platforms:Oracle Solaris...** The evaluator shall run the application while monitoring it with the utility dtrace. The evaluator shall make security-related changes to its configuration. The evaluator shall verify that dtrace logs corresponding changes to configuration files that reside in /etc (for system-specific configuration) or in the user's home directory(for user-specific configuration). **Platforms:Apple macOS...** The evaluator shall verify that the application stores and retrieves settings using the NSUserDefaults class.
Test Steps	• Locate the configuration files of the software. • Run the application and monitor it with SysInternals tool Process Monitor. • Make changes to the configuration of the application. • Verify that ProcMon logs reflect the corresponding changes to the the Windows Registry or C:\ProgramData\ directory.
Expected Test Results	• The TOE should be able to reflect the changes made to the configuration files to the Windows Registry or C:\ProgramData\ directory. • Evidence (screenshots) showing the changes made to the configuration of the TOE using Process Monitor tool. • Evidence showing that the ProcMon logs reflect the corresponding changes to the Windows Registry or C:\ProgramData\ directory.
Pass/Fail with Explanation	Pass. The Process Monitor tool reflects the changes made in the configuration of the software in the C:\ProgramData\ directory.

6.10 FMT_MEC_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	If "**implement functionality to encrypt and store configuration options as defined by FDP_PRT_EXT.1 in the PP-Module for File Encryption**" is selected, for all configuration options listed in the TSS as being stored and protected using encryption, the evaluator shall examine the contents of the configuration option storage (identified in the TSS) to determine that the options have been encrypted.
Pass/Fail with Explanation	NA. The ST does not select " **implement functionality to encrypt and store configuration options as defined by FDP_PRT_EXT.1 in the PP-Module for File Encryption**".

6.11 FPT_AEX_EXT.1.1 Test #1

Item	Data

Test Assurance Activity	The evaluator shall perform either a static or dynamic analysis to determine that no memory mappings are placed at an explicit and consistent address. The method of doing so varies per platform. For those platforms requiring the same application running on two different systems, the evaluator may alternatively use the same device. After collecting the first instance of mappings, the evaluator must uninstall the application, reboot the device, and reinstall the application to collect the second instance of mappings. **Platforms:Android...** The evaluator shall run the same application on two different Android systems. Both devices do not need to be evaluated, as the second device is acting only as a tool. Connect via ADB and inspect /proc/PID/maps. Ensure the two different instances share no memory mappings made by the application at the same location. ***Platforms:Microsoft Windows...*** *The evaluator shall run the same application on two different Windows systems and run a tool that will list all memory mapped addresses for the application. The evaluator shall then verify the two different instances share no mapping locations. The Microsoft SysInternals tool, VMMap, could be used to view memory addresses of a running application. The evaluator shall use a tool such as Microsoft's BinScope Binary Analyzer to confirm that the application has ASLR enabled.* **Platforms:Apple iOS...** The evaluator shall perform a static analysis to search for any mmap calls (or API calls that call mmap), and ensure that no arguments are provided that request a mapping at a fixed address. **Platforms:Linux...** The evaluator shall run the same application on two different Linux systems. The evaluator shall then compare their memory maps using pmap -x PID to ensure the two different instances share no mapping locations. **Platforms:Oracle Solaris...** The evaluator shall run the same application on two different Solaris systems. The evaluator shall then compare their memory maps using pmap -x PID to ensure the two different instances share no mapping locations. **Platforms:Apple macOS...** The evaluator shall run the same application on two different Mac systems. The evaluator shall then compare their memory maps using vmmap PID to ensure the two different instances share no mapping locations.
Test Steps	• Start the application on two separate platforms (identical platforms). • Run the Microsoft SysInternals tool, VMMap that will list all memory mapped addresses for the application and verify that two different instances do not share mapping locations. • Confirm that the application has ASLR enabled using Microsoft's BinScope Binary Analyzer tool.
Expected Test Results	• The application running on two different machines should not share memory mapping location. • Screenshots of VMMap tool showing that two different instances do not share mapping locations. • Screenshots showing that the application has ASLR enabled.
Pass/Fail with Explanation	Pass. It has been verified that the application running on two different platforms share no memory mapping location and ASLR is enabled. This meets testing requirements.

6.12 FPT_AEX_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	The evaluator shall verify that no memory mapping requests are made with write and execute permissions. The method of doing so varies per platform. **Platforms:Android...** The evaluator shall perform static analysis on the application to verify that mmap is never invoked with both the PROT_WRITE and PROT_EXEC permissions, and mprotect is never invoked. ***Platforms:Microsoft Windows...*** *The evaluator shall use a tool such as Microsoft's BinScope Binary Analyzer to confirm that the application passes the NXCheck. The evaluator may also ensure that the /NXCOMPAT flag was used during compilation to verify that DEP protections are enabled for the application.* **Platforms:Apple iOS...** The evaluator shall perform static analysis on the application to verify that mprotect is never invoked with the PROT_EXEC permission. **Platforms:Linux...** The evaluator shall perform static analysis on the application to verify that both mmap is never be invoked with both the PROT_WRITE and PROT_EXEC permissions, and mprotect is never invoked with the PROT_EXEC permission. **Platforms:Oracle Solaris...** The evaluator shall perform static analysis on the application to verify that both mmap is never be invoked with both the PROT_WRITE and PROT_EXEC permissions, and mprotect is never invoked with the PROT_EXEC permission. **Platforms:Apple macOS...** The evaluator shall perform static analysis on the application to verify that mprotect is never invoked with the PROT_EXEC permission.
Test Steps	• Verify that the application passes the NXCheck using Microsoft's BinScope Binary Analyzer tool which will ensure that the /NXCOMPAT flag was used during compilation to verify that DEP protections are enabled
Expected Test Results	• The application should pass the NXCheck using Microsoft's BinScope Binary Analyzer tool which will ensure that the /NXCOMPAT flag was used during compilation to verify that DEP protections are enabled. • Screenshot of Microsoft's BinScope Binary Analyzer tool showing that NXCheck is passed.
Pass/Fail with Explanation	Pass. It has been verified that the application passes the NXCheck using Microsoft's BinScope Binary Analyzer tool which will ensure that the /NXCOMPAT flag was used during compilation to verify that DEP protections are enabled.

6.13 FPT_AEX_EXT.1.3 Test #1

Item	Data
Test Assurance Activity	The evaluator shall configure the platform in the ascribed manner and carry out one of the prescribed tests: **Platforms:Android...** Applications running on Android cannot disable Android security features, therefore this requirement is met and no evaluation activity is required. ***Platforms:Microsoft Windows...*** *If the OS platform supports Windows Defender Exploit Guard (Windows 10 version 1709 or later), then the evaluator shall ensure that the application can run successfully with*

	Windows Defender Exploit Guard Exploit Protection configured with the following minimum mitigations enabled; Control Flow Guard (CFG), Randomize memory allocations (Bottom-Up ASLR), Export address filtering (EAF), Import address filtering (IAF), and Data Execution Prevention (DEP). The following link describes how to enable Exploit Protection, https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/customize-exploit-protection. *If the OS platform supports the Enhanced Mitigation Experience Toolkit (EMET) which can be installed on Windows 10 version 1703 and earlier, then the evaluator shall ensure that the application can run successfully with EMET configured with the following minimum mitigations enabled; Memory Protection Check, Randomize memory allocations (Bottom-Up ASLR), Export address filtering (EAF), and Data Execution Prevention (DEP).* **Platforms:Apple iOS...** Applications running on iOS cannot disable security features, therefore this requirement is met and no evaluation activity is required. **Platforms:Linux...** The evaluator shall ensure that the application can successfully run on a system with either SELinux or AppArmor enabled and in enforce mode. **Platforms:Oracle Solaris...** The evaluator shall ensure that the application can run with Solaris Trusted Extensions enabled and enforcing. **Platforms:Apple macOS...** The evaluator shall ensure that the application can successfully run on macOS without disabling any security features.
Test Steps	• Start the TOE application service. • Enable Windows Defender Exploit Guard Exploit Protection configured with the following minimum mitigations enabled; Control Flow Guard (CFG), Randomize memory allocations (Bottom-Up ASLR), Export address filtering (EAF), Import address filtering (IAF), and Data Execution Prevention (DEP). • Ensure that the application can run successfully with Windows Defender Exploit Guard.
Expected Test Results	• The TOE should run successfully with Windows Defender Exploit Guard. • Screenshots showing the following minimum mitigations are enabled; Control Flow Guard (CFG), Randomize memory allocations (Bottom-Up ASLR), Export address filtering (EAF), Import address filtering (IAF), and Data Execution Prevention (DEP). • Screenshots showing that the application runs successfully with the listed mitigations enabled.
Pass/Fail with Explanation	Pass. It has been verified that the application runs successfully with Windows Defender Exploit Guard Exploit Protection after enabling the specified mitigations.

6.14 FPT_AEX_EXT.1.4 Test #1

Item	Data
Test Assurance Activity	The evaluator shall run the application and determine where it writes its files. For files where the user does not choose the destination, the evaluator shall check whether the destination directory contains executable files. This varies per platform: **Platforms:Android...** The evaluator shall run the program, mimicking normal usage, and note where all user-modifiable files are written. The evaluator shall ensure that there are no executable files stored under /data/data/package/ where package is the Java package of the application. ***Platforms:Microsoft Windows...***

	For Windows Universal Applications the evaluator shall consider the requirement met because the platform forces applications to write all data within the application working directory (sandbox). For Windows Desktop Applications the evaluator shall run the program, mimicking normal usage, and note where all user-modifiable files are written. The evaluator shall ensure that there are no executable files stored in the same directories to which the application wrote user-modifiable files. **Platforms:Apple iOS...** The evaluator shall consider the requirement met because the platform forces applications to write all data within the application working directory (sandbox). **Platforms:Linux...** The evaluator shall run the program, mimicking normal usage, and note where all user-modifiable files are written. The evaluator shall ensure that there are no executable files stored in the same directories to which the application wrote user-modifiable files. **Platforms:Oracle Solaris...** The evaluator shall run the program, mimicking normal usage, and note where all user-modifiable files are written. The evaluator shall ensure that there are no executable files stored in the same directories to which the application wrote user-modifiable files. **Platforms:Apple macOS...** The evaluator shall run the program, mimicking normal usage, and note where all user-modifiable files are written. The evaluator shall ensure that there are no executable files stored in the same directories to which the application wrote user-modifiable files.
Test Steps	• Start the TOE application service. • Run the application and list user-modifiable files opened by TOE application. • List the directories of the user-modifiable files from above step. • Verify that no executable files are stored in the same directories to which the application wrote user-modifiable files.
Expected Test Results	• Verify that no executable files are stored in the same directories to which the application wrote user-modifiable files. • Evidence (screenshots) showing the location where all user-modifiable files are written. • Evidence (screenshots) showing that executable files are not stored in the same directory to which the application wrote user-modifiable files.
Pass/Fail with Explanation	Pass. It has been verified that the executable files are not stored in the same directories to which the application wrote user-modifiable files.

6.15 FPT_AEX_EXT.1.5 Test #1

Item	Data
Test Assurance Activity	The evaluator will inspect every native executable included in the TOE to ensure that stack-based buffer overflow protection is present. ***Platforms:Microsoft Windows...*** *Applications that run as Managed Code in the .NET Framework do not require these stack protections. Applications developed in Object Pascal using the Delphi IDE compiled with RangeChecking enabled comply with this element. For other code, the evaluator shall review the TSS and verify that the /GS flag was used during compilation. The evaluator shall run a tool like, BinScope, that can verify the correct usage of /GS.* **For PE** , the evaluator will disassemble each and ensure the following sequence appears: mov rcx, QWORD PTR [rsp+(...)] xor rcx, (...)

	call (...) **For ELF executables**, the evaluator will ensure that each contains references to the symbol __stack_chk_fail. Tools such as Canary Detector may help automate these activities.
Test Steps	• Verify that the application has stack-based buffer overflow protection enabled from the TSS. • Run the Microsoft's BinScope Binary Analyzer tool to check whether /GS flag was used during compilation.
Expected Test Results	• The application should have stack-based buffer overflow protection enabled . • Screenshot from the TSS showing that stack-based buffer overflow protection is enabled. • Screenshot from Microsoft's BinScope Binary Analyzer tool showing that GSCheck is passed to verify that /GS flag was used.
Pass/Fail with Explanation	Pass. It has been verified that stack-based buffer overflow protection is present and /GS flag was used during compilation of the application.

6.16 FPT_IDV_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall install the application, then check for the existence of version information. If SWID tags is selected the evaluator shall check for a .swidtag file. The evaluator shall open the file and verify that is contains at least a SoftwareIdentity element and an Entity element.
Test Steps	• Start the TOE application. • Go to the System Settings by clicking on the gear icon located on the upper right of the application. Click on **"About"** section to display the version information of AppDetectivePRO. Note: SWID tags are not supported by TOE according to ST.
Expected Test Results	• The application should have the correct version information. • Evidence (screenshots) showing that the application has the correct version.
Pass/Fail with Explanation	Pass. The Application has the correct version information.

6.17 FPT_LIB_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall install the application and survey its installation directory for dynamic libraries. The evaluator shall verify that libraries found to be packaged with or employed by the application are limited to those in the assignment.
Test Steps	• Verify the status of the installed application. • Survey the installation directory for dynamic libraries. • Compare the listed libraries and verify that libraries found to be packaged with or employed by the application are limited to those in the assignment.
Expected Test Results	• The dynamic libraries packaged with or employed by the application should be limited to those in the assignment. • Evidence (screenshots) showing dynamic libraries in the installation directory of the application.

	• Evidence (screenshots) showing the dynamic libraries packaged with or employed by the application are limited to those in the assignment.
Pass/Fail with Explanation	Pass. It is verified that the dynamic libraries packaged with or employed by the application are limited to those in the assignment.

6.18 FDP_NET_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall run the application. While the application is running, the evaluator shall sniff network traffic ignoring all non-application associated traffic and verify that any network communications witnessed are documented in the TSS or are user-initiated.
Test Steps	• Run the application. • Verify that the network communications witnessed are user-initiated and capture the network traffic via packet capture.
Expected Test Results	• The application network communications should be user initiated. • Evidence (Packet capture, screenshots) showing that the witnessed network communications are user-initiated.
Pass/Fail with Explanation	Pass. It has been verified that the network communications witnessed are user-initiated.

6.19 FDP_NET_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall run the application. After the application initializes, the evaluator shall run network port scans to verify that any ports opened by the application have been captured in the ST for the third selection and its assignment. This includes connection-based protocols (e.g. TCP, DCCP) as well as connectionless protocols (e.g. UDP).
Pass/Fail with Explanation	NA because the ST does not claim that the TOE respond to any remotely initiated communication.

6.20 FTP_DIT_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall exercise the application (attempting to transmit data; for example by connecting to remote systems or websites) while capturing packets from the application. The evaluator shall verify from the packet capture that the traffic is encrypted with HTTPS, TLS, DTLS, SSH, or IPsec in accordance with the selection in the ST.
Pass/Fail with Explanation	N/A. The TOE does not transmit any sensitive data.

6.21 FTP_DIT_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall exercise the application (attempting to transmit data; for example by connecting to remote systems or websites) while capturing packets from the application. The evaluator shall review the packet capture and verify that no sensitive data is transmitted in the clear.
Pass/Fail with Explanation	N/A. The TOE does not transmit any sensitive data.

6.22 FTP_DIT_EXT.1.1 Test #3

Item	Data
Test Assurance Activity	The evaluator shall inspect the TSS to determine if user credentials are transmitted. If credentials are transmitted the evaluator shall set the credential to a known value. The

	evaluator shall capture packets from the application while causing credentials to be transmitted as described in the TSS. The evaluator shall perform a string search of the captured network packets and verify that the plaintext credential previously set by the evaluator is not found.
Pass/Fail with Explanation	NA. No credentials are being transmitted.

6.23 FMT_SMF.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall test the application's ability to provide the management functions by configuring the application and testing each option selected from above. The evaluator is expected to test these functions in all the ways in which the ST and guidance documentation state the configuration can be managed.
Test Steps	• List the management functions specified by the ST. • Test the above management functions as per the ST.
Expected Test Results	• The TOE should be able to provide the management functions as specified in the ST. • Screenshots showing the management functions listed in the ST. • Screenshots showing the management functions are tested successfully as per the ST.
Pass/Fail with Explanation	Pass. The management functions of the TOE have been tested successfully as per the ST and guidance documentation.

6.24 FPR_ANO_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	If **require user approval before executing is selected**, the evaluator shall run the application and exercise the functionality responsibly for transmitting PII and verify that user approval is required before transmission of the PII.
Pass/Fail with Explanation	NA. The ST does not select "**require user approval before executing".**

6.25 FCS_RBG_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	If **invoke platform-provided DRBG functionality** is selected, the following tests shall be performed The evaluator shall decompile the application binary using a decompiler suitable for the application (TOE). The evaluator shall search the output of the decompiler to determine that, for each API listed in the TSS, that API appears in the output. If the representation of the API does not correspond directly to the strings in the following list, the evaluator shall provide a mapping from the decompiled text to its corresponding API, with a description of why the API text does not directly correspond to the decompiled text and justification that the decompiled text corresponds to the associated API. The following are the per-platform list of acceptable APIs: **Platforms:Android...** The evaluator shall verify that the application uses at least one of javax.crypto.KeyGenerator class or the java.security.SecureRandom class or /dev/random or /dev/urandom.

	Platforms:Microsoft Windows... *The evaluator shall verify that rand_s, RtlGenRandom, BCryptGenRandom, or CryptGenRandom API is used for classic desktop applications. The evaluator shall verify the application uses the RNGCryptoServiceProvider class or derives a class from System.Security.Cryptography.RandomNumberGenerator API for Windows Universal Applications. It is only required that the API is called/invoked, there is no requirement that the API be used directly. In future versions of this document, CryptGenRandom may be removed as an option as it is no longer the preferred API per vendor documentation.* **Platforms:Apple iOS...** The evaluator shall verify that the application invokes either SecRandomCopyBytes, CCRandomGenerateBytes, or CCRandomCopyBytes, or uses /dev/random directly to acquire random. **Platforms:Linux...** The evaluator shall verify that the application collects random from /dev/random or /dev/urandom. **Platforms:Oracle Solaris...** The evaluator shall verify that the application collects random from /dev/random. **Platforms:Apple macOS...** The evaluator shall verify that the application invokes either CCRandomGenerateBytes or CCRandomCopyBytes, or collects random from /dev/random. If invocation of platform-provided functionality is achieved in another way, the evaluator shall ensure the TSS describes how this is carried out, and how it is equivalent to the methods listed here (e.g. higher-level API invokes identical low-level API).
Pass/Fail with Explanation	NA. The ST does not select "**invoke platform-provided DRBG functionality** ".

6.26 FDP_DEC_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	**Platforms:Android...** The evaluator shall verify that each uses-permission entry in the AndroidManifest.xml file for access to a hardware resource is reflected in the selection. ***Platforms:Microsoft Windows...*** *For Windows Universal Applications the evaluator shall check the WMAppManifest.xml file for a list of required hardware capabilities. The evaluator shall verify that the user is made aware of the required hardware capabilities when the application is first installed. This includes permissions such as ID_CAP_ISV_CAMERA, ID_CAP_LOCATION, ID_CAP_NETWORKING, ID_CAP_MICROPHONE, ID_CAP_PROXIMITY and so on. A complete list of Windows App permissions can be found at: http://msdn.microsoft.com/en-US/library/windows/apps/jj206936.aspx* *For Windows Desktop Applications the evaluator shall identify in either the application software or its documentation the list of the required hardware resources.* **Platforms:Apple iOS...** The evaluator shall verify that either the application or the documentation provides a list of the hardware resources it accesses. **Platforms:Linux...** The evaluator shall verify that either the application software or its documentation provides a list of the hardware resources it accesses. **Platforms:Oracle Solaris...** The evaluator shall verify that either the application software or its documentation provides a list of the hardware resources it accesses.

	Platforms:Apple macOS... The evaluator shall verify that either the application software or its documentation provides a list of the hardware resources it accesses.
Test Steps	• List the required hardware resources as per the ST. • Verify the list of hardware resources in the documentation provided.
Expected Test Results	• The hardware resources mentioned in ST should be verified with those in the documentation provided. • Screenshot showing hardware resources mentioned in the ST. • Screenshot showing hardware resources mentioned in the Guidance Document.
Pass/Fail with Explanation	Pass. The resources accessed mentioned in the ST were verified with those in the documentation provided.

6.27 FDP_DEC_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	**Platforms:Android...** The evaluator shall verify that each uses-permission entry in the AndroidManifest.xml file for access to a sensitive information repository is reflected in the selection. ***Platforms:Microsoft Windows...*** *For Windows Universal Applications the evaluator shall check the WMAppManifest.xml file for a list of required capabilities. The evaluator shall identify the required information repositories when the application is first installed. This includes permissions such as ID_CAP_CONTACTS,ID_CAP_APPOINTMENTS,ID_CAP_MEDIALIB and so on. A complete list of Windows App permissions can be found at:* *http://msdn.microsoft.com/en-US/library/windows/apps/jj206936.aspx* *For Windows Desktop Applications the evaluator shall identify in either the application software or its documentation the list of sensitive information repositories it accesses.* **Platforms:Apple iOS...** The evaluator shall verify that either the application software or its documentation provides a list of the sensitive information repositories it accesses. **Platforms:Linux...** The evaluator shall verify that either the application software or its documentation provides a list of sensitive information repositories it accesses. **Platforms:Oracle Solaris...** The evaluator shall verify that either the application software or its documentation provides a list of sensitive information repositories it accesses. **Platforms:Apple macOS...** The evaluator shall verify that either the application software or its documentation provides a list of sensitive information repositories it accesses.
Pass/Fail with Explanation	NA. The TOE does not access sensitive information repositories.

6.28 FPT_API_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall then compare the list with the supported APIs (available through e.g. developer accounts, platform developer groups) and ensure that all APIs listed in the TSS are supported.
Test Steps	• List the APIs used in the TOE as mentioned in the ST - Section 6 – TSS.

	• Compare the above list with the supported APIs through developer accounts or platform developer groups.
Expected Test Results	• The APIs included in the ST should be mentioned in the Platform Developer webpages.
Pass/Fail with Explanation	Pass. It has been verified that the API's mentioned in the ST are supported.

6.29 FPT_TUD_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall check for an update using procedures described in either the application documentation or the platform documentation and verify that the application does not issue an error. If it is updated or if it reports that no update is available this requirement is considered to be met.
Test Steps	• Check for current version of application. • Check for available update using procedures described in application documentation and verify that the application does not issue an error.
Expected Test Results	• The TOE should not generate any error while checking for an Update. • Screenshot showing the current version of the application. • Screenshot showing the available updates for the application.
Pass/Fail with Explanation	Pass. TOE does not generate any error while checking for an Update. This meets the testing requirements.

6.30 FPT_TUD_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	The evaluator shall query the application for the current version of the software according to the operational user guidance. The evaluator shall then verify that the current version matches that of the documented and installed version.
Test Steps	• Start the TOE. • Check the version of TOE application. • Verify current version matches the documented version.
Expected Test Results	• The current version of the TOE should match with that of the documented and installed version. • Screenshot showing the version information present in the application. • Screenshot showing the version information present in the ST.
Pass/Fail with Explanation	Pass. It has been verified that the current version of the TOE matches with the installed and documented version.

6.31 FPT_TUD_EXT.1.3 Test #1

Item	Data
Test Assurance Activity	The evaluator shall verify that the application's executable files are not changed by the application. **Platforms:Apple iOS...** The evaluator shall consider the requirement met because the platform forces applications to write all data within the application working directory (sandbox).

	***For all other platforms**, the evaluator shall perform the following test:* *The evaluator shall install the application and then locate all of its executable files. The evaluator shall then, for each file, save off either a hash of the file or a copy of the file itself. The evaluator shall then run the application and exercise all features of the application as described in the ST. The evaluator shall then compare each executable file with the either the saved hash or the saved copy of the files. The evaluator shall verify that these are identical.*
Test Steps	• Install the TOE and then locate its executable file. • Generate hashed copy of the executable file. • Run the application. • Generate hashed copy of the executable file and compare hashes before and after application is run.
Expected Test Results	• Hash of all the executable files should be verified to be identical before and after running the application. • Evidence (screenshots) showing the executable files of the application. • Evidence (screenshots) showing the hashed copy of executable files before and after running the application. • Evidence (screenshots) showing that hash of all executable files before & after running the application are identical.
Pass/Fail with Explanation	Pass. It is verified that the hashed copy of the executable file is same before and after running the application.

6.32 FPT_TUD_EXT.1.5 TSS #1

Item	Data
Test Assurance Activity	The evaluator shall verify that the TSS identifies how the application is distributed. If "**with the platform**" is selected the evaluated shall perform a clean installation or factory reset to confirm that TOE software is included as part of the platform OS. If "**as an additional package**" is selected the evaluator shall perform the tests in FPT_TUD_EXT.2.
Pass/Fail with Explanation	This testing is covered by the requirements in FPT_TUD_EXT.2.

6.33 FPT_TUD_EXT.2.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall verify that application updates are distributed in the format supported by the platform. This varies per platform: **Platforms:Android...** The evaluator shall ensure that the application is packaged in the Android application package (APK) format. ***Platforms:Microsoft Windows...*** *The evaluator shall ensure that the application is packaged in the standard Windows Installer (.MSI) format, the Windows Application Software (.EXE) format signed using the Microsoft Authenticode process, or the Windows Universal Application package (.APPX) format. See https://msdn.microsoft.com/en-us/library/ms537364(v=vs.85).aspx for details regarding Authenticode signing.* **Platforms:Apple iOS...** The evaluator shall ensure that the application is packaged in the IPA format. **Platforms:Linux...**

	The evaluator shall ensure that the application is packaged in the format of the package management infrastructure of the chosen distribution. For example, applications running on Red Hat and Red Hat derivatives shall be packaged in RPM format. Applications running on Debian and Debian derivatives shall be packaged in DEB format. **Platforms:Oracle Solaris...** The evaluator shall ensure that the application is packaged in the PKG format. **Platforms:Apple macOS...** The evaluator shall ensure that application is packaged in the DMG format, the PKG format, or the MPKG format.
Test Steps	• Verify that the application is packaged in the Windows Application Software (.EXE) format. • Show the digital signature details of the application and verify that it is signed using a trusted entity.
Expected Test Results	• The application should be packaged in the Windows Application Software (.EXE) format. • Screenshot showing the digital signature of the software.
Pass/Fail with Explanation	Pass. It has been verified that the application is packaged in the Windows Application Software (.EXE) format signed using a verified entity.

6.34 FPT_TUD_EXT.2.2 Test #1

Item	Data
Test Assurance Activity	**All Other Platforms…** The evaluator shall record the path of every file on the entire filesystem prior to installation of the application, and then install and run the application. Afterwards, the evaluator shall then uninstall the application, and compare the resulting filesystem to the initial record to verify that no files, other than configuration, output, and audit/log files, have been added to the filesystem. **TD0664 has been applied.**
Test Steps	• Record the path of every file on the entire filesystem prior to installing the TOE and save the output. • Install the TOE. • Start the application and confirm the application is running after configuration. • Uninstall the TOE. • Record the path of every file on the entire filesystem, save the output and verify that no files, other than configuration, output, and audit/log files, have been added to the filesystem.
Expected Test Results	• No files other than configuration, output, and audit/log files should be added to the filesystem. • Evidence (screenshots) showing the path of every file on the filesystem before installing the TOE. • Evidence (screenshots) showing no files, other than configuration, output, and audit/log files were added to the filesystem after the application was uninstalled.
Pass/Fail with Explanation	Pass. It has been verified that the path prior to installing the application and after the application is uninstalled is same and no files, other than configuration, output, and audit/log files, have been added to the filesystem.

7 Security Assurance Requirements

7.1 AGD_OPE.1 Operational User Guidance

7.1.1 AGD_OPE.1

7.1.1.1 AGD_OPE.1 Guidance 1

Objective	If cryptographic functions are provided by the TOE, the operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.
Evaluator Findings	The evaluator examined the AGD and determined that cryptographic functions are not provided by the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.1.1.2 AGD_OPE.1 Guidance 2

Objective	The documentation must describe the process for verifying updates to the TOE by verifying a digital signature – this may be done by the TOE or the underlying platform. The evaluator shall verify that this process includes the following steps: • Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory). • Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes generation of the digital signature. The TOE will likely contain security functionality that does not fall in the scope of evaluation under this PP. The operational guidance shall make it clear to an administrator which security functionality is covered by the evaluation activities.
Evaluator Findings	The evaluator examined the section titled **"Installation"**, sub-section **"Install AppDetectivePRO"** in the AGD to verify that it describes the process for verifying updates to the TOE by verifying a digital signature. Upon investigation, the evaluator found that the AGD states that: **"Download the official AppDetectivePRO 10.2 software from the Support section in Trustwave's Fusion Customer Portal at https://fusion.trustwave.com/. The SHA1 hash is provided to customers with the product announcement and can be used to validate the integrity of the installer. Specific details around licensing and obtaining customer support can be referenced in sections 1.4.3 and 1.6 respectively.** **Updates to AppDetectivePRO 10.2 are performed using the same installer as fresh installations. This installer is signed with a code signing certificate issued by a trusted Certificate Authority and is verified by Windows before installation."** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2 AGD_PRE.1 Preparative Procedures

7.2.1 AGD_PRE.1

7.2.1.1 AGD_PRE.1 Guidance 1

Objective	As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms claimed for the TOE in the ST.
Evaluator Findings	The evaluator examined the section titled **1.2 Typical System Requirements** in the AGD to verify that it adequately addresses all platforms claimed for the TOE in the ST. Upon investigation, the evaluator found that the AGD identifies each of the platforms. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3 ALC Assurance Activities

7.3.1 ALC_CMC.1

7.3.1.1 ALC_CMC.1 TSS 1

Objective	The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST.
Evaluator Findings	The evaluator examined the section titled **Security Target and TOE Reference** in the Security Target to verify that the Security Target and TOE Reference contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Upon investigation, the evaluator found that TOE is identified as follows: **Category** / **Identifier** TOE Identifier: Trustwave AppDetectivePRO TOE Version: V10.2 TOE Developer: Trustwave Holdings Inc. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.1.2 ALC_CMC.1 TSS 2

Objective	If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.
Evaluator Findings	The evaluator examined the vendor web site to ensure that the information in the ST is sufficient to distinguish the product. Upon investigation, the evaluator found that the information on the TOE can be found at vendor's website. https://www.trustwave.com/en-us/services/database-security/appdetectivepro/

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.1.3 ALC_CMC.1 Guidance 1

Objective	Further, the evaluator shall check the AGD guidance to ensure that the version number is consistent with that in the ST.
Evaluator Findings	The evaluator examined the **Cover page** in the AGD to verify that the version number is consistent with that in the ST. Upon investigation, the evaluator found that the AGD states that the TOE is: Version 10.2 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.2 ALC_CMS.1

7.3.2.1 ALC_CMS.1 Guidance 1

Objective	The evaluator shall ensure that the developer has identified (in guidance documentation for application developers concerning the targeted platform) one or more development environments appropriate for use in developing applications for the developer's platform. For each of these development environments, the developer shall provide information on how to configure the environment to ensure that buffer overflow protection mechanisms in the environment(s) are invoked (e.g., compiler flags). The evaluator shall ensure that this documentation also includes an indication of whether such protections are on by default, or have to be specifically enabled.
Evaluator Findings	The evaluator examined the section titled "**AppDetectivePRO Basics"**, sub-sections **"Typical System Requirements"** *and* **"Supported Database Platforms"** in the platform developer guidance documentation to verify that it identifies one or more development environments appropriate for use in developing applications for the developer's platform. For each of these development environments, the evaluator verified that the developer it provides information on how buffer overflow protection mechanisms in the environments are invoked. Upon investigation, the evaluator found that the section titled **"Installation"**, sub-section **"Install AppDetectivePRO"** in the guidance documentation states that: **"Windows 10 environments for AppDetectivePRO installations already have buffer overflow protection mechanisms enabled by default. For more information on how to verify these settings, consult: https://learn.microsoft.com/en-us/windows/security/threat-protection/overview-of-threat-mitigations-in-windows-10#data-execution-prevention." .** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.2.2 ALC_CMS.1 Guidance 2

Objective	The evaluator shall ensure that the TSF is uniquely identified (with respect to other products from the TSF vendor), and that documentation provided by the developer in association with the requirements in the ST is associated with the TSF using this unique identification.

Evaluator Findings	The evaluator examined the section titled **1 AppDetectivePRO Basics** in the AGD to verify that it is associated with the TSF using unique identification. Upon investigation, the evaluator found that the guidance documentation states that: AppDetectivePRO is an in-depth database security assessment solution. It provides a comprehensive database security diagnostics approach that includes vulnerability assessment, configuration assessment, and identity access assessment. The solution provides easy to use features that allow you to get up and running quickly. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.3 ALC_TSU.1

7.3.3.1 ALC_TSU.1 TSS 1

Objective	The evaluator shall verify that the TSS contains a description of the timely security update process used by the developer to create and deploy security updates. The evaluator shall verify that this description addresses the entire application. The evaluator shall also verify that, in addition to the TOE developer's process, any third-party processes are also addressed in the description. The evaluator shall also verify that each mechanism for deployment of security updates is described.
Evaluator Findings	The evaluator examined the section titled **TOE Summary Specification** in the Security Target to verify that the TSS contains a description of the timely security update process that addresses the entire application (including third-party processes). Upon investigation, the evaluator found that the TSS states that: Trustwave provides regular product releases throughout the year. These releases contain bug fixes and security updates for ADP and third-party components. Customers are notified when a release is made available. Release notes identify the security vulnerabilities that are fixed in the release. The evaluator also examined the section titled **TOE Summary Specification** in the Security Target to verify that each mechanism for deployment of security updates is described. Upon investigation, the evaluator found that the TSS states that: The only mechanism to deploy security updates is through regular releases (every 90 days). Upon discovery of a vulnerability, the impact will be assessed for priority and scheduled for the next available release based on the complexity of the fix required. Mitigation of third-party component vulnerabilities will depend on availability of the remediation and will be scheduled for inclusion into a release as soon as they become available. All security reports are communicated from customers to Product Support through the Trustwave Fusion Support Portal. For anonymous public reporting Trustwave provides an HTTPS site that allows submissions of bugs or vulnerability reports to the product team. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.3.2 ALC_TSU.1 TSS 2

Objective	The evaluator shall verify that, for each deployment mechanism described for the update process, the TSS lists a time between public disclosure of a vulnerability and public availability

	of the security update to the TOE patching this vulnerability, to include any third-party or carrier delays in deployment. The evaluator shall verify that this time is expressed in a number or range of days.
Evaluator Findings	The evaluator examined the section titled **TOE Summary Specification** in the Security Target to verify that, for each deployment mechanism described for the update process, the TSS lists a time between public disclosure of a vulnerability and public availability of the security update to the TOE patching this vulnerability. Upon investigation, the evaluator found that the TSS states that: The only mechanism to deploy security updates is through regular releases (every 90 days). Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.3.3 ALC_TSU.1 TSS 3

Objective	The evaluator shall verify that this description includes the publicly available mechanisms (including either an email address or website) for reporting security issues related to the TOE. The evaluator shall verify that the description of this mechanism includes a method for protecting the report either using a public key for encrypting email or a trusted channel for a website.
Evaluator Findings	The evaluator examined the section titled **TOE Summary Specification** in the Security Target to verify that the TSS includes the publicly available mechanisms for reporting security issues related to the TOE, including a method for protecting the report. Upon investigation, the evaluator found that the TSS states that: Trustwave customers can submit support issues through the Fusion portal (https://fusion.trustwave.com/). This is an HTTPS website that requires user authentication. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.4 AVA_VAN.1 Vulnerability Survey

7.4.1 AVA_VAN.1

7.4.1.1 AVA_VAN.1 Activity 1 **[Labgram #116]**

Objective	The evaluator shall document their analysis and testing of potential vulnerabilities with respect to this requirement. The evaluator documents the sources consulted and the vulnerabilities found in the report.
Evaluator Findings	The evaluator documented their analysis and testing of potential vulnerabilities with respect to this requirement. Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included protocols, TOE software version, and TOE hardware to ensure sufficient coverage under AVA. The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below. • http://nvd.nist.gov/ • http://www.us-cert.gov

	• http://www.securityfocus.com/ • https://www.cvedetails.com/ The evaluator performed the public domain vulnerability searches using the following key words. The search was performed on September 08,2023 • 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 evaluator selected the search key words based upon the following criteria. • The vendor name was searched, • The product name was searched, • Key platform features the product leverages were searched, including frameworks, runtime environments, operating systems, processors, cryptographic libraries, and • Third-party libraries upon which the TOE depends for its function. Based upon the analysis, any issues found were patched in the TOE version and prior versions, mitigating the risk factor. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.4.1.2 AVA_VAN.1 Activity 2 **[TD0554]**

Objective	**Conditional for Windows, Linux, macOS and Solaris:** The evaluator shall also run a virus scanner with the most current virus definitions against the application files and verify that no files are flagged as malicious.
Evaluator Findings	The evaluator documented their analysis and testing of potential malicious files with respect to this requirement. The evaluator performed the virus scans using Avast Antivirus with the latest virus definitions. The scan was performed on 12th June 2023. Based upon the analysis, no malicious files were identified. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

8 Conclusion

The testing shows that all test cases required for conformance have passed testing.

End of Document