Trustwave AppDetectivePRO v10.2 Security Target

Document Version: 1.9

2400 Research Blvd
Suite 395
Rockville, MD 20850

Revision History:

Version	Date	Changes
Version 1.0	04/12/2022	Initial official release
Version 1.1	05/01/2022	Updated to conform to APPcPPv1.4
Version 1.2	05/02/2022	Addressed internal review comments
Version 1.3	07/30/2022	Addressed ECR comments – Updated figure 1.
Version 1.4	17/03/2023	ST updated in accordance with multiple new NIAP TDs
Version 1.5	31/03/2023	Minor update to table 2
Version 1.6	21/07/2023	Multiple updates in section 2.3.1 and section 6
Version 1.7	11/08/2023	Update to section 2.3.1
Version 1.8	08/09/2023	Update to section 2.3.1
Version 1.9	20/09/2023	Update to section 1.4.3

Contents

1 Introduction

The Security Target (ST) serves as the basis for the Common Criteria (CC) evaluation and identifies the Target of Evaluation (TOE), the scope of the evaluation, and the assumptions made throughout. This document will also describe the intended operational environment of the TOE, and the functional and assurance requirements that the TOE meets.

1.1 Product Description

Trustwave AppDetectivePRO is a database and big data scanner the identifies configuration mistakes, identification and access control issues, missing patches, and any toxic combination of settings that could lead to escalation of privilege attacks, data leakage, denial-of-service (Dos), or unauthorized modification of data held within data stores.

With a simple setup and an easy-to-use interface, you can discover, assess, and report on the security, risk, or compliance posture of any database or big data store within your environment – on premise or in the cloud – in minutes. AppDetectivePRO is an excellent addition to any existing security toolkit with its focus on relationship databases and big data stores. It complements host/network operating systems and static/dynamic application scanners.

AppDetectivePRO enables users to:

- Leverage a solution that is quick to deploy and easy to use, with low hardware requirements.
- Access easy to use built-in regulatory policies or create custom policies to match specific business needs.
- Gain insight into your auditors' findings by using the database tool most frequently used by them.
- Improve your database security posture with auditing and identify your privileged users with user rights review.

1.2 Security Target and TOE Reference

This section provides the information needed to identify and control the TOE and the ST.

Table 1 – TOE/ST Identification

Category	Identifier
ST Title	Trustwave AppDetectivePRO v10.2 Security Target
ST Version	1.9
ST Date	09/20/2023
ST Author	Acumen Security, LLC.
TOE Identifier	Trustwave AppDetectivePRO
TOE Version	v10.2
TOE Developer	Trustwave Holdings Inc.
Key Words	Database, DBMS, Application Software

1.3 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.

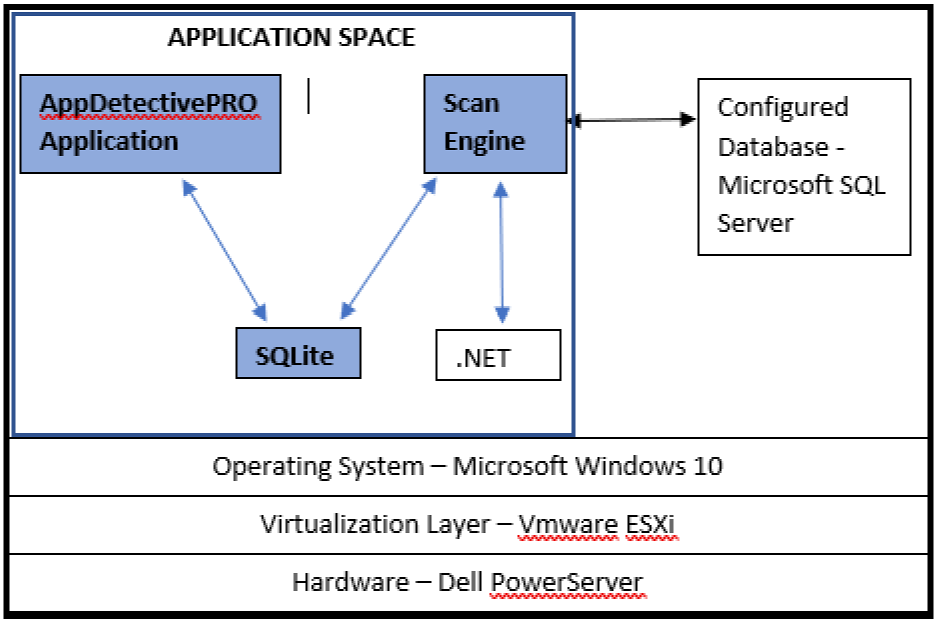
1.4 TOE Description

AppDetectivePRO is application software executing on a Microsoft Windows 10 platform. Configuration information is stored in a backend SQLite (v3.35.5) database. .NET is a required component of the Operational Environment.

1.4.1 Physical Boundaries

The TOE is application software that resides entirely within the application space of a Microsoft Windows 10 instance. The physical boundaries of the TOE are illustrated in Figure 1. TOE components are shown with blue shading.

Figure 1 – TOE Boundaries


APPLICATION SPACE
AppDetectivePRO Application
Scan Engine
Configured Database - Microsoft SQL Server
SQLite
.NET
Operating System – Microsoft Windows 10
Virtualization Layer – Vmware ESXi
Hardware – Dell PowerServer

1.4.2 Security Functions Provided by the TOE

The TOE provides the security functions described in the following sections.

1.4.2.1 Cryptographic Support

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

1.4.2.2 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.

1.4.2.3 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.

1.4.2.4 Privacy

The TOE itself does not contain or transmit any PII.

1.4.2.5 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.

1.4.2.6 Trusted Path/Channels

The TOE does not transmit sensitive data.

1.4.3 TOE Documentation

The following documents are essential to understanding and controlling the TOE in the evaluated configuration:

- Trustwave AppDetectivePRO User Guide, Version 10.2

1.5 TOE Environment

The following environmental components are required to operate the TOE in the evaluated configuration:

Table 2 – Required Environmental Components

Component	Required	Purpose/Description
.NET	Yes	Framework 4.8
Java Runtime Environment	Yes	Java SE 8 Java Runtime Environment (JRE)
Operating System	Yes	Microsoft Windows 10 (64-bit)
Virtualization	Yes	VMware ESXi v6.x (v6.7 used in this evaluation)
Hardware	Yes	Minimum requirements are: • 8 GB RAM • Dual core x64 Processor, 1.6 GHz (Intel Xeon Gold 6126 (Skylake) used in this evaluation) • 7 GB of available disk space

Component	Required	Purpose/Description
Scanned Databases	Yes	A supported remote database that is scanned by the TOE. • Microsoft SQL (version 2017) is used for the evaluation.

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. The node-locked license is generated by the order fulfilment team of Trustwave is sent separately via email.

1.6 Product Functionality not Included in the Scope of the Evaluation

The following product functionality is not included in the CC evaluation:

- ASAP Updates
- The following database types:
    - IBM DB2 LUW
    - Oracle
    - SAP (Sybase) ASE
    - MySQL
    - PostgreSQL
    - Hadoop
    - Microsoft Azure SQL Database
    - Teradata
    - MongoDB
    - SAP HANA
    - Couchbase
    - MariaDB
    - Elasticsearch
    - Percona Server for MySQL

2 Conformance Claims

This section identifies the TOE conformance claims, conformance rationale, and relevant Technical Decisions (TDs).

2.1 CC Conformance Claims

The TOE is conformant to the following:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017 Extended
- Common Criteria for Information Technology Security Evaluations Part 3, Version 3.1, Revision5, April 2017 Extended

2.2 Protection Profile Conformance

This ST also claims exact conformance to the following:

- NIAP Protection Profile for Application Software, Version 1.4, 2021-10-07 [APP-PP]

2.3 Conformance Rationale

This Security Target provides exact conformance to the items listed in the previous section. The security problem definition, security objectives, and security requirements in this ST are all taken from the Protection Profile (PP), performing only the operations defined there.

2.3.1 Technical Decisions

All NIAP Technical Decisions (TDs) issued to date and applicable to [APP-PP] have been addressed, as necessary. Table 3 identifies all applicable TDs.

Table 3 – Relevant Technical Decisions

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0780: FIA_X509_EXT.1 Test 4 Clarification	No	The TOE does not support transmit any encrypted data
TD0756: Update for platform-provided full disk encryption	Yes	
TD0747: Configuration Storage Option for Android	No	The TOE is not an application that runs on Android
TD0743: FTP_DIT_EXT.1.1 Selection exclusivity	Yes	
TD0736: Number of elements for iterations of FCS_HTTPS_EXT.1	No	The TOE does not support transmit any encrypted data using HTTPS
TD0719: ECD for PP APP V1.3 and 1.4	Yes	
TD0717: Format changes for PP_APP_V1.4	Yes	

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0664: Testing activity for FPT_TUD_EXT.2.2	Yes	
TD0650: Conformance claim sections updated to allow for MOD_VPNC_V2.3 and 2.4	Yes	This is a PP_APP_v1.4 update which is applicable to this ST. However, the TOE does not have any claims to include MOD_VPNC_V2.4.
TD0628: Addition of Container Image to Package Format	Yes	

3 Security Problem Definition

The security problem definition is taken directly from the claimed PP and any relevant EPs/Modules/Packages specified in Section 2.2 and is reproduced here for the convenience of the reader. The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any Organizational Security Policies (OSPs) that the TOE is expected to enforce.

3.1 Threats

The threats included in Table 4 are drawn directly from the PP specified in Section 2.2.

Table 4 – Threats

ID	Threat
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.

3.2 Assumptions

The assumptions included in Table 5 are drawn directly from PP.

Table 5 – Assumptions

ID	Assumption
A.PLATFORM	The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.

3.3 Organizational Security Policies

No Organizational Security Policies (OSPs) apply to the TOE.

4 Security Objectives

The security objectives have been taken directly from the claimed and are reproduced here for the convenience of the reader.

4.1 Security Objectives for the TOE

The security objectives in the following table apply to the TOE.

Table 6 – Security Objectives

ID	Security Objectives
O.INTEGRITY	Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom, if ever, shipped without errors. The ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options.
O.QUALITY	To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs.
O.MANAGMENT	To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII.
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data.
O.PROTECTED_COMMS	To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs will use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application.

4.2 Security Objectives for the Operational Environment

Security objectives for the operational environment assist the TOE in correctly providing its security functionality. These objectives, which are found in the table below, track with the assumptions about the TOE operational environment.

Table 7 – Security Objectives for the Operational Environment

ID	Objectives for the Operational Environment
OE.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.
OE.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.
OE.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

5 Security Requirements

This section identifies the Security Functional Requirements (SFRs) for the TOE. The SFRs included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, September 2017, and all international interpretations.

Table 8 – SFRs

Requirement	Description
FCS_CKM_EXT.1	Cryptographic Key Generation Services
FCS_RBG_EXT.1	Random Bit Generation Services
FCS_STO_EXT.1	Storage of Credentials
FDP_DEC_EXT.1	Access to Platform Resources
FDP_NET_EXT.1	Network Communications
FDP_DAR_EXT.1	Encryption of Sensitive Application Data
FMT_CFG_EXT.1	Secure by Default Configuration
FMT_MEC_EXT.1	Supported Configuration Mechanism
FMT_SMF.1	Specification of Management Functions
FPR_ANO_EXT.1	User Consent for Transmission of Personally Identifiable Information
FPT_AEX_EXT.1	Anti-Exploitation Capabilities
FPT_API_EXT.1	Use of Supported Services and APIs
FPT_IDV_EXT.1	Software Identification and Versions
FPT_LIB_EXT.1	Use of Third Party Libraries
FPT_TUD_EXT.1	Integrity for Installation and Update
FPT_TUD_EXT.2	Integrity for Installation and Update
FTP_DIT_EXT.1	Protection of Data in Transit

5.1 Conventions

The CC allows the following types of operations to be performed on the functional requirements: assignments, selections, refinements, and iterations. The following font conventions are used within this document to identify operations defined by CC:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with <u>underlined</u> text;
- Iteration: Indicated by appending the iteration identifier in parenthesis, e.g., (1), (2), (3).
- Where operations were completed in the PP and relevant EPs/Modules/Packages, the formatting used in the PP has been retained.
- Extended SFRs are identified by the addition of "EXT" after the requirement name.

5.2 Security Functional Requirements

This section includes the security functional requirements for this ST.

5.2.1 Cryptographic Support (FCS)

5.2.1.1 FCS_CKM_EXT.1 Cryptographic Key Generation Services

FCS_CKM_EXT.1.1

The application shall [

- generate no asymmetric cryptographic keys,

].

Application Note: Modified in accordance with TD0717

5.2.1.2 FCS_RBG_EXT.1 Random Bit Generation Services

FCS_RBG_EXT.1.1

The application shall [

- use no DRBG functionality

] for its cryptographic operations.

5.2.1.3 FCS_STO_EXT.1 Storage of Credentials

FCS_STO_EXT.1.1

The application shall [

- not store any credentials.

] to non-volatile memory.

5.2.2 User Data Protection (FDP)

5.2.2.1 FDP_DAR_EXT.1 Encryption of Sensitive Application Data

FDP_DAR_EXT.1.1

The application shall [

- leverage platform-provided functionality to encrypt sensitive data,

] in non-volatile memory.

5.2.2.2 FDP_DEC_EXT.1 Access to Platform Resources

FDP_DEC_EXT.1.1

The application shall restrict its access to [

- network connectivity,

].

FDP_DEC_EXT.1.2

The application shall restrict its access to [

- no sensitive information repositories,

].

5.2.2.3 FDP_NET_EXT.1 Network Communications

FDP_NET_EXT.1.1

The application shall restrict network communication to [

- user-initiated communication for [*scanning configured databases*].

].

5.2.3 Security Management (FMT)

5.2.3.1 FMT_MEC_EXT.1 Supported Configuration Mechanism

FMT_MEC_EXT.1.1

The application shall [

- *invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.*]

5.2.3.2 FMT_CFG_EXT.1 Secure by Default Configuration

FMT_CFG_EXT.1.1

The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

FMT_CFG_EXT.1.2

The application shall be configured by default with file permissions which protect the application binaries and data files from modification by normal unprivileged users.

5.2.3.3 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions [

- *[Session management; Asset management; System Settings management; Policy management]*

].

5.2.4 Privacy (FPR)

5.2.4.1 FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information

FPR_ANO_EXT.1.1

The application shall [

- not transmit PII over a network,

].

5.2.5 Protection of the TSF (FPT)

5.2.5.1 FPT_AEX_EXT.1 Anti-Exploitation Capabilities

FPT_AEX_EXT.1.1

The application shall not request to map memory at an explicit address except for [*no exceptions*].

FPT_AEX_EXT.1.2

The application shall [

- *not allocate any memory region with both write and execute permissions* ,

].

FPT_AEX_EXT.1.3

The application shall be compatible with security features provided by the platform vendor.

FPT_AEX_EXT.1.4

The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

FPT_AEX_EXT.1.5

The application shall be built with stack-based buffer overflow protection enabled.

5.2.5.2 FPT_API_EXT.1 Use of Supported Services and APIs

FPT_API_EXT.1.1

The application shall use only documented platform APIs.

5.2.5.3 FPT_IDV_EXT.1 Software Identification and Versions

FPT_IDV_EXT.1.1

The application shall be versioned with [*[Major.Minor.Incremental]*] .

5.2.5.4 FPT_LIB_EXT.1 Use of Third Party Libraries

FPT_LIB_EXT.1.1

The application shall be packaged with only [

- *pkg:generic/AWSSDK.Core@3.3.103.7*
- *pkg:generic/AWSSDK.RDS@3.3.107.0*
- *pkg:generic/Antlr3.Runtime@3.5.1*
- *pkg:generic/AppDetectivePRO.resources@10.2.3690.3*
- *pkg:generic/AppSecInc.Checks.Contracts@1.23.0.0*
- *pkg:generic/AppSecInc.Checks.KnowledgeBase@1.0.0.0*
- *pkg:generic/AppSecInc.Checks.Service.Core@1.29.1598.5*
- *pkg:generic/AppSecInc.Data.Drivers@1.0.24.0*

- *pkg:generic/AppSecInc.Data.Drivers@1.1.25.0*
- *pkg:generic/AppSecInc.DatabaseSchema@1.39.966.3*
- *pkg:generic/AppSecInc.Discovery.Contracts@1.12.0.0*
- *pkg:generic/AppSecInc.Logging@1.15.0.46*
- *pkg:generic/AppSecInc.Madison.AppScanProxy.WSEData@1.0.0.0*
- *pkg:generic/AppSecInc.Madison.BL.resources@10.2.3690.3*
- *pkg:generic/AppSecInc.Madison.Presentation.UserRights@10.2.3690.3*
- *pkg:generic/AppSecInc.Madison.Presentation.UserRights.resources@10.2.3690.3*
- *pkg:generic/AppSecInc.Madison.ScanEngine@10.2.3690.3*
- *pkg:generic/AppSecInc.ProcessDomain@1.10.0.0*
- *pkg:generic/AppSecInc.ScanEngine.Contracts@3.0.0.0*
- *pkg:generic/AppSecInc.ScanEngine.ExpressionEvaluator@1.15.0.46*
- *pkg:generic/AppSecInc.ScanEngine.Logging.Remote@1.15.0.46*
- *pkg:generic/AppSecInc.ScanEngine.Logging@3.13.1076.10*
- *pkg:generic/AppSecInc.Service.Core@1.27.695.5*
- *pkg:generic/AppSecInc.UserRights.Contracts@4.10.0.0*
- *pkg:generic/AppSecInc.UserRights.Service@1.39.966.3*
- *pkg:generic/AppSecInc.Util.RangeMap@1.1.0.33*
- *pkg:generic/AppSecInc.Wcf.WsdlExtensions.Exceptions@1.1.0.0*
- *pkg:generic/AppSecInc.Wcf.WsdlExtensions.Flatten@1.0.0.0*
- *pkg:generic/AutoMapper@7.0.0*
- *pkg:generic/BucklerCore@5.11.3.1122*
- *pkg:generic/BucklerWinUtils@1.0.0.0*
- *pkg:generic/ChecksResources@1.29.1598.5*
- *pkg:generic/CommandLine@2.2.1*
- *pkg:generic/Common.Logging.Core@3.4.1*
- *pkg:generic/Common.Logging@3.4.1*
- *pkg:generic/Couchbase.NetClient@2.7.10*
- *pkg:generic/CryptoManaged@1.0.0.0*
- *pkg:generic/DevExpress.Charts.v20.2.Core@20.2.6.0*
- *pkg:generic/DevExpress.CodeParser.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Data.Desktop.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Data.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Data.v20.2.resources@20.2.6.0*
- *pkg:generic/DevExpress.DataAccess.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.DataAccess.v20.2.resources@20.2.6.0*
- *pkg:generic/DevExpress.DataVisualization.v20.2.Core@20.2.6.0*
- *pkg:generic/DevExpress.Diagram.v20.2.Core@20.2.6.0*
- *pkg:generic/DevExpress.Images.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Mvvm.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Office.v20.2.Core@20.2.6.0*
- *pkg:generic/DevExpress.Office.v20.2.Core.resources@20.2.6.0*
- *pkg:generic/DevExpress.Pdf.v20.2.Core@20.2.6.0*
- *pkg:generic/DevExpress.Pdf.v20.2.Core.resources@20.2.6.0*
- *pkg:generic/DevExpress.Pdf.v20.2.Drawing@20.2.6.0*
- *pkg:generic/DevExpress.PivotGrid.v20.2.Core@20.2.6.0*

- *pkg:generic/DevExpress.PivotGrid.v20.2.Core.resources@20.2.6.0*
- *pkg:generic/DevExpress.Printing.v20.2.Core@20.2.6.0*
- *pkg:generic/DevExpress.Printing.v20.2.Core.resources@20.2.6.0*
- *pkg:generic/DevExpress.RichEdit.v20.2.Core@20.2.6.0*
- *pkg:generic/DevExpress.RichEdit.v20.2.Core.resources@20.2.6.0*
- *pkg:generic/DevExpress.RichEdit.v20.2.Export@20.2.6.0*
- *pkg:generic/DevExpress.Sparkline.v20.2.Core@20.2.6.0*
- *pkg:generic/DevExpress.Sparkline.v20.2.Core.resources@20.2.6.0*
- *pkg:generic/DevExpress.TreeMap.v20.2.Core@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Accordion.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Charts.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Charts.v20.2.resources@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.CodeView.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Controls.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Controls.v20.2.resources@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Core.v20.2.Extensions@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Core.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Core.v20.2.resources@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.DataAccess.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Diagram.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Docking.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Docking.v20.2.resources@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.DocumentViewer.v20.2.Core@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.DocumentViewer.v20.2.Core.resources@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.ExpressionEditor.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Grid.v20.2.Core@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Grid.v20.2.Core.resources@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Grid.v20.2.Extensions@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Grid.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Layout.v20.2.Core@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.LayoutControl.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.LayoutControl.v20.2.resources@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.NavBar.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.NavBar.v20.2.resources@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Office.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.PdfViewer.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.PdfViewer.v20.2.resources@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.PivotGrid.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Printing.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Printing.v20.2.resources@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.PropertyGrid.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Ribbon.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Ribbon.v20.2.resources@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.RichEdit.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.RichEdit.v20.2.resources@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Themes.ADProTheme.v20.2@20.2.6.0*

- *pkg:generic/DevExpress.Xpf.Themes.Office2016White.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.Themes.Office2019Colorful.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpf.TreeMap.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpo.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.Xpo.v20.2.resources@20.2.6.0*
- *pkg:generic/DevExpress.XtraCharts.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.XtraCharts.v20.2.resources@20.2.6.0*
- *pkg:generic/DevExpress.XtraGauges.v20.2.Core@20.2.6.0*
- *pkg:generic/DevExpress.XtraGauges.v20.2.Core.resources@20.2.6.0*
- *pkg:generic/DevExpress.XtraReports.v20.2@20.2.6.0*
- *pkg:generic/DevExpress.XtraReports.v20.2.resources@20.2.6.0*
- *pkg:generic/Devart.Data.Universal.MySql@3.80.2227.0*
- *pkg:generic/Devart.Data.Universal.Oracle@3.80.2227.0*
- *pkg:generic/Devart.Data.Universal.PostgreSql@3.80.2227.0*
- *pkg:generic/Devart.Data.Universal@3.80.2227.0*
- *pkg:generic/Devart.Data@5.0.2522.0*
- *pkg:generic/DnsClient@1.4.0*
- *pkg:generic/Elasticsearch.Net@7.8.0*
- *pkg:generic/FirebirdSql.Data.FirebirdClient@4.6.0.0*
- *pkg:generic/FluentNHibernate@3.1.0*
- *pkg:generic/Iesi.Collections@4.0.0*
- *pkg:generic/Iesi.Collections@4.0.4*
- *pkg:generic/IronPython@2.7.11.1000*
- *pkg:generic/NGenerics@1.3.0.0*
- *pkg:generic/NHibernate@4.1.1*
- *pkg:generic/NHibernate@5.3.8*
- *pkg:generic/Nest@7.8.0*
- *pkg:generic/Ninject@3.0.0.15*
- *pkg:generic/Nito.AsyncEx.Enlightenment@4.0.1*
- *pkg:generic/Nito.AsyncEx@4.0.1*
- *pkg:generic/OpenTracing@0.12.0*
- *pkg:generic/PostSharp@2.1.6.11*
- *pkg:generic/PresentationFramework.Aero@4.8.3761.0*
- *pkg:generic/Prism.Unity.Wpf@8.0.0.1909*
- *pkg:generic/Prism.Wpf@8.0.0.1909*
- *pkg:generic/Prism@8.0.0.1909*
- *pkg:generic/QueryADataset@1.0.0.83*
- *pkg:generic/Remotion.Linq.EagerFetching@2.2.0*
- *pkg:generic/Remotion.Linq@2.2.0*
- *pkg:generic/SharpCompress@0.23.0*
- *pkg:generic/SmartThreadPool@2.2.1.0*
- *pkg:generic/System.Buffers@4.6.28619.01*
- *pkg:generic/System.Data.SQLite@1.0.112.1*
- *pkg:generic/System.Data.SQLite@1.0.110.0*
- *pkg:generic/System.Diagnostics.DiagnosticSource@4.6.26919.02*
- *pkg:generic/System.Runtime.CompilerServices.Unsafe@4.6.26919.02*

- *pkg:generic/System.Threading.Tasks.Extensions@4.6.27129.04*
- *pkg:generic/System.Windows.Interactivity@3.0.40218.0*
- *pkg:generic/Unity.Abstractions@5.11.6*
- *pkg:generic/Unity.Container@5.11.8*
- *pkg:generic/WeOnlyDo.Client.SSH.FIPS@2.6.5.165*
- *pkg:generic/WeOnlyDo.Client.SSH@2.6.5.165*
- *pkg:generic/log4net@2.0.12.0*
- *pkg:generic/websocket-sharp@1.0.4.0*

].

5.2.5.5 FPT_TUD_EXT.1 Integrity for Installation and Update

FPT_TUD_EXT.1.1

The application shall [leverage the platform] to check for updates and patches to the application software.

FPT_TUD_EXT.1.2

The application shall [provide the ability] to query the current version of the application software.

FPT_TUD_EXT.1.3

The application shall not download, modify, replace or update its own binary code.

FPT_TUD_EXT.1.4

Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.

FPT_TUD_EXT.1.5

The application is distributed [as an additional software package to the platform OS]

5.2.5.6 FPT_TUD_EXT.2 Integrity for Installation and Update

FPT_TUD_EXT.2.1

The application shall be distributed using [the format of the platform-supported package manager].

Application note: modified in accordance with TD0628.

FPT_TUD_EXT.2.2

The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

FPT_TUD_EXT.2.3

The application installation package shall be digitally signed such that its platform can cryptographically verify them prior to installation.

5.2.6 Trusted Path/Channel (FTP)

5.2.6.1 FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.1.1

The application shall [

- not transmit any [sensitive data]

] between itself and another trusted IT product.

5.3 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the PP and any relevant EPs/Modules/Packages, which is/are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in Table 9.

Table 9 – Security Assurance Requirements

Assurance Class	Assurance Components	Component Description
Security Target	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security problem definition
Development	ADV_FSP.1	Basic functionality specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative user guidance
Life Cycle Support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
	ALC_TSU.1	Timely Security Updates
Tests	ATE_IND.1	Independent testing – conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability survey

5.4 Assurance Measures

The TOE satisfied the identified assurance requirements. This section identifies the Assurance Measures applied by Trustwave to satisfy the assurance requirements. The following table lists the details.

Table 10 TOE Security Assurance Measures

SAR Component	How the SAR will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any

SAR Component	How the SAR will be met
	security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes).
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated.
ALC_CMS.1	
ALC_TSU_EXT.1	This component requires the TOE developer, in conjunction with any other necessary parties, to provide information as to how the end-user devices are updated to address security issues in a timely manner. The documentation describes the process of providing updates to the public from the time a security flaw is reported/discovered, to the time an update is released. This description includes the parties involved (e.g., the developer, carriers(s)) and the steps that are performed (e.g., developer testing, carrier testing), including worst case time periods, before an update is made available to the public.
ATE_IND.1	Vendor will provide the TOE for testing.
AVA_VAN.1	Vendor will provide the TOE for testing. Vendor will provide a document identifying the list of software and hardware components.

6 TOE Summary Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 11 – TOE Summary Specification SFR Description

Requirement	TSS Description
ALC_TSU.1_EXT.1	Trustwave customers can submit support issues through the Fusion portal (https://fusion.trustwave.com/). This is an HTTPS website that requires user authentication. 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 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.
FCS_CKM_EXT.1	The TOE does not generate any asymmetric keys.
FCS_RBG_EXT.1	The TOE does not use any DRBG functionality.
FCS_STO_EXT.1	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.
FDP_DAR_EXT.1	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. ADP runs on drives with Windows Bitlocker enabled to protect all data at rest.
FDP_DEC_EXT.1	The TOE accesses network connectivity and no sensitive information repositories.
FDP_NET_EXT.1	Network connections occur for scanning of user-configured databases.
FMT_CFG_EXT.1	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 userid 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 userid of the person performing the installation is automatically configured as the only authorized

Requirement	TSS Description
	Administrator. That Administrator may execute the application and add other userids 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.
FMT_MEC_EXT.1	ADP stores configuration data under the ProgramData directory.
FMT_SMF.1	ADP provides functionality for authorized users to manage Sessions (which include Assets), System Settings, and Policies.
FPR_ANO_EXT.1	The TOE does not transmit PII over the network.
FPT_AEX_EXT.1	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.
FPT_API_EXT.1	The TOE uses the following platform APIs: • Microsoft.Expression.Interactions.dll • Microsoft.dynamic.dll • Microsoft.scripting.dll • Microsoft.SqlServer.Types.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.
FPT_IDV_EXT.1	The TOE uses “Major.Minor.Incremental” versioning.
FPT_LIB_EXT.1	The third-party libraries incorporated into the TOE are listed in section 5.2.5.4.
FPT_TUD_EXT.1 FPT_TUD_EXT.2	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. All updates to ADP are provided through the Fusion customer portal for download. A SHA1 hash is also provided to the customers to validate the downloaded files.

Requirement	TSS Description
	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. 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.
FTP_DIT_EXT.1	The TOE does not transmit sensitive data.`

7 Acronym Table

Table 12 – Acronyms

Acronym	Definition
API	Application Programming Interface
AppSW	Application Software Protection Profile
ASLR	Address Space Layout Randomization
CA	Certificate Authority
CC	Common Criteria
CRL	Certificate Revocation List
DoS	Denial of Service
DPAPI	Data Protection Application Programming Interface
DRBG	Deterministic Random Bit Generator
EKU	Extended Key Usage
EP	Extended Package
GB	GigaByte
GUI	Graphical User Interface
JRE	Java Runtime Environment
NIAP	Nation Information Assurance Partnership
OCSP	Online Certificate Status Protocol
PP	Protection Profile
RAM	Random Access Memory
SFR	Security Functional Requirement
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSS	TOE Summary Specification