Trustwave AppDetectivePRO Version 8.7 Security Target

Version 1.10

February 13, 2017

Trustwave
70 West Madison Street
Suite 1050
Chicago, IL 60602

DOCUMENT INTRODUCTION

Prepared By:

Common Criteria Consulting LLC
15804 Laughlin Lane
Silver Spring, MD 20906
http://www.consulting-cc.com

Prepared For:

Trustwave
70 West Madison Street
Suite 1050
Chicago, IL 60602
http://www.trustwave.com

REVISION HISTORY

Rev	Description
1.0	March 17, 2014, Initial release
1.1	May 28, 2014, Addressed lab ORs/CRs
1.2	July 20, 2014, Addressed certifier ORs/CRs
1.3	August 5, 2014, Addressed certifier ORs/CRs
1.4	September 1, 2014, Added FAU_SAR
1.5	March 10, 2015, Updated guidance documentation
1.6	June 10, 2015, Updated SFR
1.7	June 23, 2015, Modified the evaluated databases
1.8	June 26, 2015, Added the build number
1.9	July 16, 2015, Adjusted the DBs supported for scanning
1.10	February 13, 2017, Updates for Assurance Maintenance

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

CC ..... **Common Criteria**
DBMS ..... **DataBase Management System**
EAL ..... **Evaluation Assurance Level**
GB ..... **GigaByte**
GHz ..... **Giga-Hertz**
IDS ..... **Intrusion Detection System**
IIS ..... **Internet Information Services**
IP ..... **Internet Protocol**
IT ..... **Information Technology**
MB ..... **MegaByte**
OS ..... **Operating System**
OSP ..... **Organisational Security Policy**
PP ..... **Protection Profile**
RAM ..... **Random Access Memory**
SFR ..... **Security Functional Requirement**
ST ..... **Security Target**
TOE ..... **Target of Evaluation**
TSF ..... **TOE Security Function**

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Trustwave AppDetectivePRO Version 8.7. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1*. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

Trustwave AppDetectivePRO Version 8.7 Security Target, Version 1.10, dated February 13, 2017.

1.2 TOE Reference

Trustwave AppDetectivePRO Version 8.7 (Build 2731)

1.3 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) augmented by ALC_FLR.2 from the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 4.

1.4 TOE Overview

1.4.1 Usage and Major Security Features

The TOE is a database security assessment solution that includes vulnerability assessment, configuration assessment, and identity access assessment. The TOE helps to identify vulnerable databases residing within the network by scanning for potential security vulnerabilities within those databases.

Users that have logged into Windows invoke the AppDetectivePRO application to interact with the TOE. If the user has not been authorized in the TOE, an error message is displayed and the application exits.

Once the TOE is invoked, users may operate in three distinct areas: policies, sessions, and system settings. The policies area enables a user to configure the checks to be performed for each of the defined policies. The sessions area defines the assets (databases) to be scanned and their associated policies, and also enables users to view scan results. The system settings area is used to authorize users of the TOE. Sessions and policies are shared between the authorized users of the TOE.

Each session includes a set of assets, which may be dynamically discovered or manually added. Scans may be run against selected assets within a session. Policies may be specified for audit and penetration test scans, or a rights review can be performed to capture and analyze the rights granted to database users. Once scans have been performed, the results can be reviewed interactively. A second option for reviewing results is to generate reports, which may also be saved for later review.

The TOE comprises a set of Windows applications and services. The AppDetectivePRO application presents the user interface; the services are used during discovery and scan operations.

AppDetectivePRO can generate fix scripts, customized based on scan results, which an administrator can review and apply to address identified vulnerabilities. This functionality is not included in the evaluation.

The product includes an update function (ASAP Update). Since use of this function could update the TOE to an unevaluated version, this function is not included in the evaluation.

1.5 TOE type

Data Protection

1.6 Required Non-TOE Hardware/Software/Firmware

The TOE consists of applications and services installed on a Windows system. The following minimum requirements must be satisfied by the workstation.

Table 1 - Windows System Minimum Requirements

Item	Minimum Requirements
Operating System	Windows 7 SP1
Processor	Dual core processors 1.60 GHz
RAM	3GB
Hard Drive	400 MB of free disk space for installation 5GB and higher for scan data storage
Networking	One network interface
Web Server (Console only)	IIS
Backend Database	Microsoft SQL Server 2012 (Standard or Express editions)
.NET	Microsoft .NET Framework 4.6 (automatically installed with the TOE)

The TOE stores configuration information and scan results in a backend database. The backend database may be collocated with the TOE or resident on a separate server (in the Operational Environment). If the database is collocated, the system must satisfy the minimum requirements of both the TOE and the DBMS.

The Operational Environment provides the DBMS instances to be scanned by the TOE. The TOE is capable of scanning the DBMSs in the following table. Requirements for the systems hosting the DBMSs are dependent on the DBMS type. For some DBMS types, additional drivers must be installed on their systems to enable some functions. Specific requirements are provided in the *AppDetectivePRO User Guide (v 8.7).*

Table 2 - Supported DBMSs

DBMS	Versions
Oracle (SID)	11gR2, 11gR1
Microsoft SQL Server (Instance)	2012
Sybase ASE (Dataserver)	15.7, 15.5, 15.0
IBM DB2 LUW (Database)	9.7, 9.5, 9.1
MySQL (Server)	5.5, 5.1
Hadoop (Node)	1

The TOE components depend on Windows to protect their executables and stored data images (e.g., files and registry keys) and their executing environments. The TOE also depends on the environment to ensure the Backend Database is secure. The Operational Environment must protect communication between:

- the TOE and the backend database
- the TOE and DBMS instances being scanned.

1.7 TOE Description

An operational TOE consists of one instance of the TOE installed on a Windows system.

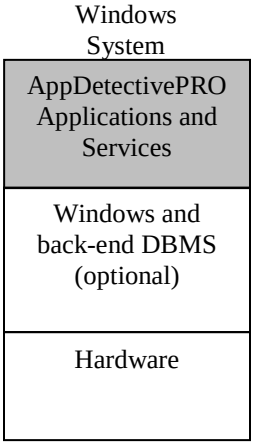
The TOE allows the authorized administrator to perform the scans described previously as well as examining scan results.

Logically, the TOE operates as a single application though it is instantiated in a series of processes utilizing inter-process communication mechanisms provided by Windows to communicate with one another.

1.7.1 Physical Boundary

The physical boundary of the TOE includes the Console and Scan Engine applications and services executing on dedicated Windows systems. The operating systems and DBMSs are not included in the TOE boundary. In the following figure, the shaded items are within the TOE boundary.

Figure 1 - Physical Boundary



The physical scope of the TOE also includes the following guidance documentation:

1. *Trustwave AppDetectivePRO* 8.7 *User Guide* (December 1, 2016)
2. *Trustwave AppDetectivePRO Common Criteria Supplement* (v1.3)

1.7.2 Logical Boundary

1.7.2.1 Database Discovery and Scanning

The TOE discovers and scans databases. Scans are performed to proactively detect vulnerabilities and inappropriate permission settings.

1.7.2.2 Scan Results Review

Scan results can be viewed via the AppDetectivePRO application. The TOE can also generate reports that can be saved.

1.7.2.3 Audit Generation

The TOE has the ability to generate audit records for TOE security-relevant events, and also provides a mechanism to review the audit records. The TOE relies on the Operational Environment to provide a reliable timestamp.

1.7.2.4 Identification

AppDetectivePRO verifies that the Windows userid of the user invoking the TOE has been authorized in the TOE. Access is denied if the Windows userid is not configured as a valid user of the TOE.

1.7.2.5 Management

The TOE provides security management functions that are accessible via the AppDetectivePRO application. Users must be authorized to use the TOE.

Two types of roles are supported, as defined by the user's Windows account. Windows administrators are able to perform all management functions. Regular users are able to perform all functions except authorizing TOE users.

1.7.3 TSF Data

The following table describes the TSF data used in the TOE.

Table 3 - TSF Data Descriptions

TSF Data	Description
Assets	Define attributes of DBMSs to be scanned. Attributes include: • Name • Associated Session • Identity (IP Address/Hostname, Port, and Instance) • Type • Host OS
Policies	Define specific scan actions to be performed. Attributes include: • Name • Included Controls and Checks
Reports	Define reports generated from scan results. Attributes include: • Name • Associated Session • Information included
Sessions	Define the Sessions associated with the Console. Attributes include: • Name • Associated Assets • Associated Reports • Scan Results
Users	Define attributes for authorized users of the Console. Attributes include: • Username

1.8 Evaluated Configuration

The evaluated configuration consists of a TOE instance executing on a Windows platform.

In addition, the following configuration options must be specified to conform to the evaluated configuration:

1. ASAP Update must not be used, since it could result in installation of an unevaluated version of the product.
2. The backend database is installed on a stand-alone system or collocated with the TOE.
3. The functionality to unmask passwords is not used, since this could expose weak passwords discovered in scanned databases for exploitation. The default configuration is to not unmask passwords.

1.9 Functionality Supported But Not Evaluated

In addition to Windows 7 SP1, the following operating systems are also supported as host platforms for the TOE: Windows 8.1, Windows 10, Windows 2008 Server SP2, Windows 2008 Server R2 SP2, Windows Server 2012, and Windows Server 2012 R2.

In addition to Microsoft SQL Server 2012, Microsoft SQL Server 2008 and Microsoft SQL Server 2014 are also supported as the backend database.

In addition to the databases listed in Table 2, the following database versions are supported for scanning:

- Oracle (SID) – 12c, 10gR2, 10gR1, 9iR2
- Microsoft SQL Server (Instance) – 2016, 2014, 2008 R2, 2008, 2005, 2000
- Sybase ASE (Dataserver) – 16.0, 12.5
- IBM DB2 LUW (Database) - 10.5, 10.1
- IBM DB2 z/OS (Subsystem) - 10.1, 9.1, 8.1
- Hadoop (Node) – 2
- MySQL – 5.7, 5.6, 5.0
- Teradata – 15.10, 15, 14.10, 14
- Microsoft Azure SQL Database

Session locking functionality has been added to version 8.7, but this functionality has not been evaluated.

2. Conformance Claims

2.1 Common Criteria Conformance

Common Criteria version: Version 3.1 Revision 4, dated September 2012

Common Criteria conformance: Part 2 extended and Part 3 conformant

2.2 Security Requirement Package Conformance

EAL2 augmented by ALC_FLR.2

The TOE does not claim conformance to any security functional requirement packages.

2.3 Protection Profile Conformance

The TOE does not claim conformance to any registered Protection Profile.

3. Security Problem Definition

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the assets and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption,* threats as T.*threat* and policies as P.*policy*.

3.2 Assumptions

The specific conditions listed in the following table are assumed to exist in the TOE environment.

Table 4 - Assumptions

A.Type	Description
A.ACCESS	The TOE has access to all the databases it needs to perform its functions.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the databases the TOE monitors.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

3.3 Threats

The threats identified in the following subsections are addressed by the TOE and/or the Operational Environment.

Table 5 - Threats

T.Type	Description
T.COMDIS	An unauthorized user may attempt to disclose the data collected by the TOE by bypassing a TOE security mechanism.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected by the TOE by bypassing a security mechanism.
T.FACCNT	Unauthorized attempts to access TOE data or security functions by an unauthorized user may go undetected, potentially enabling disclosure or modification of TOE data via brute force attacks.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential vulnerability to go undetected.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected by the TOE.
T.PRIVIL	A user may gain unauthorized access to TOE security functions and data to disclose or modify TOE data.
T.SCNCFG	An unauthorized user may use data collected by the TOE to identify improper security configuration settings that exist in the databases the TOE monitors, and use this information to gain unauthorized access to those databases.

T.Type	Description
T.SCNVUL	An unauthorized user may use data collected by the TOE to identify vulnerabilities that exist in the databases the TOE monitors, and use this information to gain unauthorized access to those databases.

3.4 Organisational Security Policies

The organisational security policies (OSPs) identified in the following table are addressed by the TOE and/or the Operational Environment.

Table 6 - Organisational Security Policies

P.Type	Description
P.ACCACT	Users of the TOE shall be accountable for their actions.
P.DETECT	Configuration and vulnerability information that might be indicative of the potential for a future intrusion of a targeted IT system (database) must be collected.
P.MANAGE	The TOE shall only be managed by authorized users.

4. Security Objectives

This section identifies the security objectives of the TOE and the TOE's Operational Environment. The security objectives identify the responsibilities of the TOE and the TOE's Operational Environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the operational environment are designated as *OE.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 7 - Security Objectives for the TOE

O.Type	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.AUDITS	The TOE must be able to record audit records for data accesses and use of the primary TOE functions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDACTS	The TOE must collect and store configuration and vulnerability information that might be indicative of the potential for a future intrusion of an IT System.
O.IDENT	The TOE must be able to identify users prior to allowing access to the TOE.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data via its own interfaces.

4.2 Security Objectives for the Operational Environment

The TOE's operational environment must satisfy the following objectives.

Table 8 - Security Objectives of the Operational Environment

OE.Type	Description
OE.AUDIT	The operational environment of the TOE can audit attempts to access the TOE's stored executable image and stored data.
OE.IDAUTH	The operational environment of the TOE authenticates users prior to allowing access to TOE via its own interfaces.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with the TOE guidance.
OE.INTROP	The TOE is interoperable with the IT System it monitors and scans.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.
OE.PROTECT	The operational environment of the TOE must protect the TOE from logical attacks including unauthorized modifications and access to stored data or TOE executables.
OE.REVIEW	The operational environment of the TOE provides the capability to review the audit records.
OE.TIME	The operational environment will provide reliable timestamps to the TOE.
OE.TRANSMIT	The operational environment must protect the data transmitted between the TOE and the operational environment components.

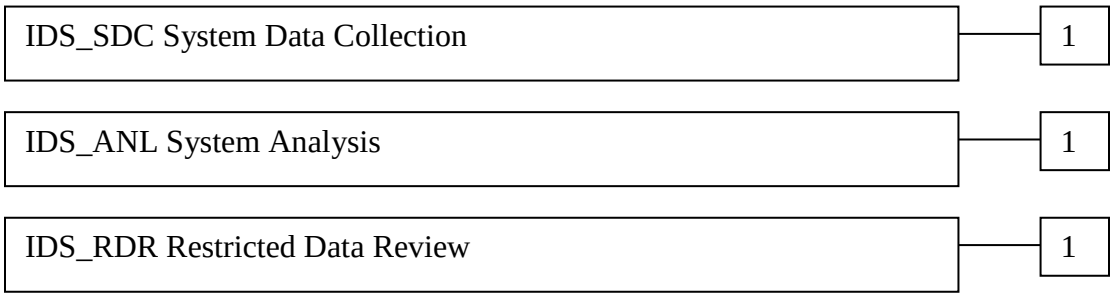
5. Extended Components Definition

5.1 Extended Security Functional Components

5.1.1 Class IDS: Intrusion Detection

All of the components in this section are based on the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments.

This class of requirements is taken from the IDS System PP to specifically address the data processed by an IDS System. The audit class of the CC (FAU) was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature of system data and provide for requirements about analyzing, reviewing and managing the data.



5.1.1.1 IDS_SDC System Data Collection

Family Behaviour:

This family defines the requirements for the TOE regarding collection of information related to security events.

Component Levelling:

IDS_SDC.1 System Data Collection provides for the functionality to require TSF controlled processing of data for database instances. The data may include database instance identification parameters (e.g. IP address), access control configuration (what user roles or permissions grant access to what data), authentication configuration (how user authentication is performed), accountability policy configuration (what audit records are generated), and user rights assignments (what roles or permissions are assigned to individual users).

Management:

The following actions could be considered for the management functions in FMT:

a) Management of the configuration information related to data collection.

Audit:

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Basic: Configuration of the information to be collected.

IDS_SDC.1 System Data Collection

Hierarchical to: No other components.

Dependencies: None

IDS_SDC.1.1 The TSF shall be able to collect and store the following information for database instances: [assignment: *data items collected*].

5.1.1.2 IDS_ANL System Analysis

Family Behaviour:

This family defines the requirements for the TOE regarding analysis of collected security events.

Component Levelling:

IDS_ANL.1 System Analysis provides for the functionality to require TSF controlled analysis of collected data.

Management:

The following actions could be considered for the management functions in FMT:

a) Configuration of the analysis to be performed.

Audit:

There are no auditable events foreseen.

IDS_ANL.1 System Analysis

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System Data Collection

IDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all collected security information:

a) [selection: *statistical*, *signature*, *integrity*, [assignment: *other analytical functions*]].

IDS_ANL.1.2 The TSF shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and

b) [assignment: *other security relevant information about the result*].

5.1.1.3 IDS_RDR Restricted Data Review

Family Behaviour:

This family defines the requirements for the TOE regarding review of the System data collected by the TOE. System data refers to the set of collected security event information together with the records generated from the analysis of the security event information.

Component Levelling:

IDS_RDR Restricted Data Review	1

IDS_RDR.1 Restricted Data Review provides for the functionality to require TSF controlled review of the System data collected by the TOE.

Management:

The following actions could be considered for the management functions in FMT:

a) Maintenance (deletion, modification, addition) of the group of users with read access right to the System data records.

Audit:

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Detailed: Reading of information from the System data records.

IDS_RDR.1 Restricted Data Review

Hierarchical to: No other components.

Dependencies: IDS_ANL.1 System Analysis

IDS_RDR.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of System data*] from the System data.

IDS_RDR.1.2 The TSF shall provide the System data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The TSF shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

5.2 Extended Security Assurance Components

None

6. Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., FAU_ARP.1(1)).

6.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation* with the exception of completed operations.

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) *Addition or removal of assets; execution of discovery scans; execution of policy scans; execution of user rights review scans.*

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *no additional information*.

6.1.1.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *all authorised users* with the capability to read all *audit information* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.2 Identification and Authentication (FIA)

6.1.2.1 FIA_UID.2 User Identification Before Any Action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3 Security Management (FMT)

6.1.3.1 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete, *and create* the *system-level data listed in the following table* to *the roles as specified in the following table*.

Table 9 - System-Level TSF Data Permissions

TSF Data	Windows Administrator	Windows User
Assets	Query, Modify, Delete, Create	Query, Modify, Delete, Create
Policies	Query, Modify, Delete, Create	Query, Modify, Delete, Create
Reports	Query, Modify, Delete, Create	Query, Modify, Delete, Create
Sessions	Query, Modify, Delete, Create	Query, Modify, Delete, Create
Users	Query, Modify, Delete, Create	Query

6.1.3.2 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- *Management of Assets,*
- *Management of Policies,*
- *Management of Reports,*
- *Management of Sessions, and*
- *Management of Users*.

6.1.3.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles *Windows Administrator and Windows User*.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.4 Intrusion Detection (IDS)

6.1.4.1 IDS_SDC.1 System Data Collection

IDS_SDC.1.1 The TSF shall be able to collect and store the following information for database instances: *Name, IP Address or Hostname, Port, Type, Host Operating System, Access Control Configuration, Authentication Configuration, Accountability Policy Configuration, and User Rights Assignments*.

6.1.4.2 IDS_ANL.1 System Analysis

IDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all collected security information:

a) *Misconfiguration, inappropriate rights assignments, and detected known vulnerabilities*.

IDS_ANL.1.2 The TSF shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and

b) *Configuration information*.

6.1.4.3 IDS_RDR.1 Restricted Data Review

IDS_RDR.1.1 The TSF shall provide *authorised users* with the capability to read *all System data* from the System data.

Application Note: "All System data" refers to the system data identified in IDS_SDC.1 or IDS_ANL.1.

IDS_RDR.1.2 The TSF shall provide the System data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The TSF shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

6.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2 augmented by ALC_FLR.2. These requirements are summarised in the following table.

Table 10 - Assurance Requirements

Assurance Class	Component ID	Component Title
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 11 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied by the Operational Environment
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied
FIA_UID.2	FIA_UID.1	None	n/a
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied
IDS_SDC.1	No other components.	None	n/a
IDS_ANL.1	No other components.	IDS_SDC.1	Satisfied
IDS_RDR.1	No other components.	IDS_ANL.1	Satisfied

7. TOE Summary Specification

7.1 Database Discovery and Scanning

The TOE is able to discover databases; they may also be manually configured. Scanning is performed against the configured databases to detect known vulnerabilities, misconfiguration, and inappropriate rights assignments (IDS_SDC.1). Information gathered about the databases is analyzed (IDS_ANL.1).

7.2 Database Review

The TOE provides authorized users with the ability to read information learned about databases in a human readable form via the AppDetectivePRO application. The information is presented through GUI interactions and Reports (IDS_RDR.1).

7.3 Audit Generation

The TOE generates audits for the events specified in FAU_GEN.1. Audit records may be viewed (FAU_SAR.1) by all authorized users via the History option within the session display of the application.

7.4 Identification

The TOE performs identification for all invocations of the AppDetectivePRO application before granting any other access (FIA_UID.2). Identities are determined from the Windows account of the invoking user. If the userid is not an authorized user of the TOE, then the user is notified via a text message and the application terminates. If valid, the role for the session is dynamically determined based on whether the userid is an authorized Windows administrator.

7.5 Management

The TOE provides management capability to enable the TOE to be controlled and monitored via the AppDetectivePRO application. Two roles are supported: Windows Administrator and Windows User (FMT_SMR.1). The specific privileges for TSF data access associated with each role are defined in FMT_MTD.1. The management functions are defined in FMT_SMF.1.

8. Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 2.

8.1 Protection Profile Reference

This Security Target does not claim conformance to any registered Protection Profile.

8.2 Protection Profile Refinements

This Security Target does not claim conformance to any registered Protection Profile.

8.3 Protection Profile Additions

This Security Target does not claim conformance to any registered Protection Profile.

8.4 Protection Profile Rationale

This Security Target does not claim conformance to any registered Protection Profile.

9. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, OSPs, assumptions and threats.

9.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each OSP, threat and assumption is addressed by a security objective.

The following table identifies for each OSP, threat and assumption, the security objective(s) that address it.

Table 12 - OSPs, Threats and Assumptions to Security Objectives Mapping

O/T/A / Objective	P.ACCACT	P.DETECT	P.MANAGE	T.COMDIS	T.COMINT	T.FACCNT	T.IMPCON	T.LOSSOF	T.PRIVIL	T.SCNCFG	T.SCNVUL	A.ACCESS	A.DYNMIC	A.MANAGE	A.NOEVIL
O.ACCESS			X	X	X		X	X	X	X	X				
O.AUDITS	X					X									
O.EADMIN			X												
O.IDACTS		X								X	X				
O.IDENT	X		X	X	X		X	X	X						
O.PROTCT			X	X	X			X	X						
OE.AUDIT						X									
OE.IDAUTH			X	X	X		X	X	X						
OE.INSTAL			X				X								X
OE.INTROP												X	X		
OE.PERSON			X										X	X	
OE.PROTECT								X	X						
OE.REVIEW	X					X									
OE.TIME	X														
OE.TRANSMIT				X	X										

9.1.1 Rationale of How Security Objectives Mapped to Threats Counter Those Threats

The following table describes the rationale for the threat to security objectives mapping.

Table 13 - Threats to Security Objectives Rationale

T.TYPE	Rationale
T.COMDIS	This Threat is satisfied by ensuring that: • O.ACCESS: The O.ACCESS objective builds upon the OE.IDAUTH objective by only permitting authorized users to access TOE data. • O.IDENT: The O.IDENT objective provides identification of users prior to any TOE function accesses. • OE.IDAUTH: The OE.IDAUTH environment objective in conjunction with O.IDENT provides authentication of users prior to any TOE access. • O.PROTCT: The O.PROTCT objective addresses this threat by providing TOE self-protection. • OE.TRANSMIT: The operational environment must protect the data transmitted between the TOE and operational environment components.
T.COMINT	This Threat is satisfied by ensuring that: • O.ACCESS: The O.ACCESS objective builds upon the OE.IDAUTH objective by only permitting authorized users to access TOE data. • O.IDENT: The O.IDENT objective provides identification of users prior to any TOE function accesses. • OE.IDAUTH: The OE.IDAUTH environment objective in conjunction with O.IDENT provides authentication of users prior to any TOE access. • O.PROTCT: The O.PROTCT objective addresses this threat by providing TOE self-protection. • OE.TRANSMIT: The operational environment must protect the data in transmit between the TOE and operational environment components.
T.FACCNT	This Threat is satisfied by ensuring that: • O.AUDITS: The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions. • OE.AUDIT: The OE.AUDIT objective ensures the operational environment of the TOE does its part in ensuring there is accountability for accessing the TOE executable and data. • OE.REVIEW: The OE.REVIEW objective supports this policy by ensuring the operational environment of the TOE provides the capability to review the generated TOE audit records.
T.IMPCON	This Threat is satisfied by ensuring that: • O.ACCESS: The O.ACCESS objective builds upon the OE.IDAUTH objective by only permitting authorized users to access TOE functions and data. • O.IDENT: The O.IDENT objective provides identification of users prior to any TOE function accesses. • OE.IDAUTH: The OE.IDAUTH environment objective in conjunction with O.IDENT provides authentication of users prior to any TOE access. • OE.INSTAL: The OE.INSTAL objective states the authorized administrators will configure the TOE properly.

T.TYPE	Rationale
T.LOSSOF	This Threat is satisfied by ensuring that: • O.ACCESS: The O.ACCESS objective builds upon the OE.IDAUTH objective by only permitting authorized users to access TOE data. • O.IDENT: The O.IDENT objective provides identification of users prior to any TOE function accesses. • OE.IDAUTH: The OE.IDAUTH environment objective in conjunction with O.IDENT provides authentication of users prior to any TOE access. • O.PROTCT: The O.PROTCT objective addresses this threat by providing TOE self-protection. • OE.PROTECT: The OE.PROTECT objective ensures that the environment provides a secure environment for the TOE.
T.PRIVIL	This Threat is satisfied by ensuring that: • O.ACCESS: The O.ACCESS objective builds upon the OE.IDAUTH objective by only permitting authorized users to access TOE functions. • O.IDENT: The O.IDENT objective provides identification of users prior to any TOE function accesses. • OE.IDAUTH: The OE.IDAUTH environment objective in conjunction with O.IDENT provides authentication of users prior to any TOE access. • O.PROTCT: The O.PROTCT objective addresses this threat by providing TOE self-protection. • OE.PROTECT: The OE.PROTECT objective ensures that the environment provides a secure environment for the TOE.
T.SCNCFG	This Threat is satisfied by ensuring that: • O.ACCESS: The O.ACCESS objective builds on O.IDACTS by requiring the results of the scans to be accessible. • O.IDACTS: The O.IDACTS objective counters this threat by requiring the TOE collect and store vulnerability information that might be indicative of a configuration setting change.
T.SCNVUL	This Threat is satisfied by ensuring that: • O.ACCESS: The O.ACCESS objective builds on O.IDACTS by requiring the results of the scans to be accessible. • O.IDACTS: The O.IDACTS objective counters this threat by requiring the TOE collect and store configuration and vulnerability information that might be indicative of a vulnerability.

9.1.2 Rationale of How Security Objectives Mapped to Assumptions Uphold Those Assumptions

The following table describes the rationale for the assumption to security objectives mapping.

Table 14 - Assumptions to Security Objectives Rationale

A.TYPE	Rationale
A.ACCESS	This Assumption is satisfied by ensuring that: • OE.INTROP: The OE.INTROP objective ensures the TOE has the needed access.
A.DYNMIC	This Assumption is satisfied by ensuring that: • OE.INTROP: The OE.INTROP objective ensures the TOE has the proper access to the IT System. • OE.PERSON: The OE.PERSON objective ensures that the TOE will be managed appropriately.

A.TYPE	Rationale
A.MANAGE	This Assumption is satisfied by ensuring that: • OE.PERSON: The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.NOEVIL	This Assumption is satisfied by ensuring that: • OE.INSTAL: The OE.INSTAL objective ensures that the TOE is properly installed and operated.

9.1.3 Rationale of How Security Objectives Mapped to OSPs Enforce Those OSPs

The following table describes the rationale for the OSP to security objectives mapping.

Table 15 - OSPs to Security Objectives Rationale

P.TYPE	Rationale
P.ACCACT	This OSP is satisfied by ensuring that: • O.AUDITS: The O.AUDITS objective implements this policy by requiring auditing of scan data accesses and use of the primary IDS TOE functions. • O.IDENT: The O.IDENT objective supports this policy by ensuring each user is uniquely identified. • OE.REVIEW: The OE.REVIEW objective supports this policy by ensuring the operational environment of the TOE provides the capability to review the generated TOE audit records. • OE.TIME: The OE.TIME objective supports this policy by ensuring a reliable time stamp is provided by the operational environment.
P.DETECT	This OSP is satisfied by ensuring that: • O.IDACTS: The O.IDACTS objective addresses this policy by requiring collection of scanned configuration and vulnerability data.
P.MANAGE	This OSP is satisfied by ensuring that: • O.ACCESS: The O.ACCESS objective builds upon the O.IDENT and OE.IDAUTH objectives by only permitting authorized users to access TOE functions. • O.EADMIN: the O.EADMIN objective ensures there is a set of functions for administrators to use. • O.IDENT: The O.IDENT objective provides identification of users prior to any TOE function accesses. • OE.IDAUTH: The OE.IDAUTH environment objective in conjunction with O.IDENT provides authentication of users prior to any TOE access. • O.PROTCT: O.PROTCT objective addresses this policy by providing TOE self-protection. • OE.INSTAL: The OE.INSTAL objective supports the O.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. • OE.PERSON: The OE.PERSON objective ensures competent administrators will manage the TOE.

9.2 Security Requirements Rationale

9.2.1 Rationale for the Security Functional Requirements Meeting the Security Objectives of the TOE

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective and the SFR(s) that address it.

Table 16 - SFRs to Security Objectives Mapping

	O.ACCESS	O.AUDITS	O.EADMIN	O.IDACTS	O.IDENT	O.PROTCT
FAU_GEN.1		X				
FAU_SAR.1		X				
FIA_UID.2					X	X
FMT_MTD.1	X					X
FMT_SMF.1			X			
FMT_SMR.1	X					
IDS_SDC.1				X		
IDS_ANL.1				X		
IDS_RDR.1	X		X			

The following table provides the rationale for the mappings identified above.

Table 17 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.ACCESS	This TOE Security Objective is satisfied by ensuring that: • FMT_MTD.1: Only authorized user can perform the management functionality associated with their role as identified in these SFRs. • FMT_SMR.1: The TOE must be able to recognize the different roles that exist for the TOE. • IDS_RDR.1: The TOE must provide the ability for authorized users to view the data collected about databases.
O.AUDITS	This TOE Security Objective is satisfied by ensuring that: • FAU_GEN.1: Security-relevant events (TOE data accesses and use of the TOE functions) must be defined and audited for the TOE. • FAU_SAR.1: The audit records may be reviewed.
O.EADMIN	This TOE Security Objective is satisfied by ensuring that: • FMT_SMF.1: The TOE must be capable of performing the security management functions. • IDS_RDR.1: The TOE must provide the ability for authorized users to view the data collected about databases.

Security Objective	SFR and Rationale
O.IDACTS	This TOE Security Objective is satisfied by ensuring that: • IDS_SDC.1: The TOE is required to collect and store vulnerability and configuration information of databases. • IDS_ANL.1: The TOE is required to analyze the databases to detect vulnerabilities and suspicious behavior.
O.IDENT	This TOE Security Objective is satisfied by ensuring that: • FIA_UID.2: The TOE requires each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.
O.PROTCT	This TOE Security Objective is satisfied by ensuring that: • FIA_UID.2: The TOE requires each user to identify itself so that users can be authorized for access. • FMT_MTD.1: Only authorized user can perform the management functionality of the TOE identified in FMT_MTD.1.

9.2.2 Security Assurance Requirements Rationale

A) Assurance of the correct functioning of the TOE to meet the security functional requirements identified in this Security Target is provided by the vendor and evaluator activities specified in the security assurance requirements. These activities are within the bounds of current best commercial practice. The evaluator review of the vendor-supplied evidence provides independent confirmation that the vendor activities have been competently performed and the certifier review of the evaluation provides assurance that the evaluator activities have been sufficiently comprehensive for the examination of the TOE and its documentation and have been done correctly.