Security Target

McAfee Database Security 4.4.3

Document Version 1.4

June 18, 2013

Prepared For:

McAfee, Inc.

2821 Mission College Blvd.

Santa Clara, CA 95054

www.mcafee.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Database Security 4.4.3. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title	Security Target: McAfee Database Security 4.4.3
ST Revision	1.4
ST Publication Date	June 18, 2013
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	McAfee Database Security 4.4.3, consisting of the following product versions: • McAfee Database Activity Monitoring Version 4.4.3 • McAfee Vulnerability Manager for Databases Version 4.4.3 • McAfee Virtual Patching for Databases Version 4.4.3
TOE Type	Database Security

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE

SECTION	TITLE	DESCRIPTION
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by *italicized* text.
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by underlined text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FIA_UAU.1.1 (1) and FIA_UAU.1.1 (2) refer to separate instances of the FIA_UAU.1 security functional requirement component.

Outside the SFRs, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

The following table describes the terms and acronyms used in this document:

TERM	DEFINITION
AD	Active Directory
CC	Common Criteria version 3.1 (ISO/IEC 15408)
CPU	Central Processing Unit
DBMS	DataBase Management System
DNS	Domain Name System
DSS	Data Security Standard
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
GUI	Graphical User Interface

TERM	DEFINITION
HTTPS	HyperText Transfer Protocol Secure
I&A	Identification & Authentication
IDS	Intrusion Detection System
IP	Internet Protocol
IT	Information Technology
JDBC	Java DataBase Connectivity
J2EE	Java 2 Platform, Enterprise Edition
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
NTP	Network Time Protocol
OEM	Original Equipment Manufacturer
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
RAM	Random Access Memory
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Mail Protocol
SOF	Strength Of Function
SP	Service Pack
SQL	Structured Query Language
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
XML	eXtensible Markup Language

Table 2 – Terms and Acronyms Used in Security Target

1.6 TOE Overview

McAfee Database Security (hereafter referred to as the Target of Evaluation) is a software solution that monitors a Database Management System (DBMS) and protects it from both internal and external threats. The TOE provides full visibility into DBMS user and application activity by way of analysis of SQL statements and queries interacting with the DBMS. Analysis of DBMS transactions is determined by a monitoring policy consisting of a set of rules (predefined and/or custom) which are configured to issue alerts and/or terminate suspicious activities. The TOE can be used in support of simple, single DBMS installations as well as complex, multi-server, multi-DBMS installations.

Rules define what types of statements are allowed to run on the DBMS, what types are forbidden, and which types should be monitored. Incoming statements are compared to the rules enabled for the

DBMS and action (allow, alert, or terminate) is taken based on the first rule that is matched. If a statement does not match any of the existing rules, the statement is allowed.

The TOE provides enhanced DBMS security based on both predefined vPatch rules and custom rules. Virtual Patching (vPatch) rules are included in the installation of the TOE (once activated with a licensed version of McAfee Virtual Patching for Databases Version 4.4) and help prevent attacks against known vulnerabilities. In addition, you can define custom rules to define the level of monitoring and alerts, and further protect the DBMS(s) against potential threats.

The major security features of the TOE include:

- Monitoring of all DBMS activities, including the activities of authorized and privileged users
- Prevention of intrusion, data theft, and other attacks on the DBMS
- Rule-based policies for users, queries and DBMS objects
- The ability to quarantine suspicious users and/or terminate user sessions
- Vulnerability assessment (VA) for monitored DBMSs

The TOE comprises of three major components:

- **McAfee Database Security Sensor**: A small-footprint process that runs on the DBMS host server. The sensor enables the monitoring of all local and network access to the DBMS(s) in real-time.
- **McAfee Database Security Server**: A J2EE server that communicates with all installed sensors. Included with the installation of the Security Server is McAfee Vulnerability Manager for Databases and Virtual Patching for Databases.[1]
- **McAfee Database Security Web Console**: A Web-based GUI dashboard that enables the administrator to review alerts, and define rules and policies.

The McAfee Database Security Sensor monitors access to the DBMS and sends all the transaction data to the McAfee Database Security Server (no data is stored on the sensors). Based on the policies defined via the McAfee Database Security Web Console, the Server logs the transaction, issues an alert, and/or prevents access to the DBMS. The external database (provided by the IT environment) stores the configuration of the system (including policy profiles of each sensor and DBMS information), alerts, VA results, audit data and other system data.

Vulnerability assessment functionality is provided by the McAfee Vulnerability Manager for Databases which enables the user to configure VA scans of the DBMSs to identify a wide range of risks and problems. VA scans use the credentials of a DBMS user and are based on predefined and/or custom tests and are driven by compliance requirements and organizational policy. McAfee Vulnerability

[1] In order to comply with the evaluated configuration, both McAfee Vulnerability Manager for Databases and Virtual Patching for Databases need to be licensed, in addition to McAfee Database Activity Monitoring. All three products comprise the TOE.

Manager for Databases is included in the installation of the Security Server component and a separate license must be purchased to activate the vulnerability assessment functionality and to comply with the evaluated configuration.

Custom reports can be fully automated, scheduled, or exported. Audit records are generated to record configuration changes made by users. The audit records may be reviewed via the GUI. The TOE requires users to identify and authenticate themselves before access is granted to any data or management functions. The TOE assigns different levels of permissions to different administrators by assigning each admin user to a specific role. Each role comprises a specific set of permissions, which are granted to those users assigned to the role.

Communication between the distributed components of the TOE (i.e. Sensor and Server) is protected from disclosure and modification by cryptographic functionality provided by the TOE.

1.7 TOE Description

The TOE helps organizations gain visibility into database activity, including local privileged access and sophisticated attacks from within the database. The TOE helps organizations protect their most valuable and sensitive data from external threats and malicious insiders. In addition to providing a reliable audit trail, the TOE also prevents intrusion by terminating sessions that violate security policy.

1.7.1 Physical Boundary

The TOE is software-only and includes:

1. **McAfee Database Security Sensor**: A small-footprint process (application) that runs on one or more DBMS host server(s). The sensor enables the monitoring of all local and network access to the DBMS(s) in real-time.

2. **McAfee Database Security Server**: A J2EE server that communicates with all installed sensors. Functionality provided by McAfee Vulnerability Manager for Databases and Virtual Patching for Databases is provided as part of the Security Server installation. The management interface of the Server is provided by the Web Console.

3. **McAfee Database Security Web Console**: A Web-based GUI dashboard that enables the administrator to review alerts, define rules and policies, and to manage vulnerability tests, scans and results. The Web Console is accessible via the McAfee Database Security Server.

The hardware, operating systems and all third party support software (e.g., DBMS) on the systems on which the TOE executes are excluded from the TOE boundary.

In order to comply with the evaluated configuration, the following hardware and software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER

TOE Software	McAfee Database Security Version 4.4.3, comprising of the following licensed software:
	• McAfee Database Activity Monitoring Version 4.4.3, including:
	  ○ McAfee Database Security Server
	  ○ McAfee Database Security Sensor
	  ○ McAfee Database Security Web Console
	• McAfee Vulnerability Manager for Databases Version 4.4.3
	• McAfee Virtual Patching for Databases Version 4.4.3

IT Environment	Specified in the following: • Table 4 – Management System Component Requirements • Table 5 – Supported DBMS Platforms • Table 6 – DBMS Platform Hardware Requirements • Table 7 – Supported DBMS Platforms for Vulnerability Assessment Functionality
TOE Guidance Documentation	The guidance for the TOE is described in the following documentation: • Security Target: McAfee Database Security 4.4.3 (this document) • Operational User Guidance and Preparative Procedures Supplement: McAfee Database Security 4.4.3 • McAfee Database Security User's Guide • McAfee Database Security Installation Guide

Table 3 – Evaluated Configuration for the TOE

The evaluated configuration consists of a single instance of the management system (with the McAfee Database Security Server accessible via the McAfee Database Security Web Console interface) and one or more instances of the sensor software monitoring the DBMSs (with McAfee Database Security Sensor). McAfee Vulnerability Manager for Databases and Virtual Patching for Databases are integrated components of McAfee Database Security Server that must be licensed to comply with the evaluated configuration.

The following figure presents an example of an operational configuration. The shaded elements in the boxes at the top of the figure represent the TOE components.

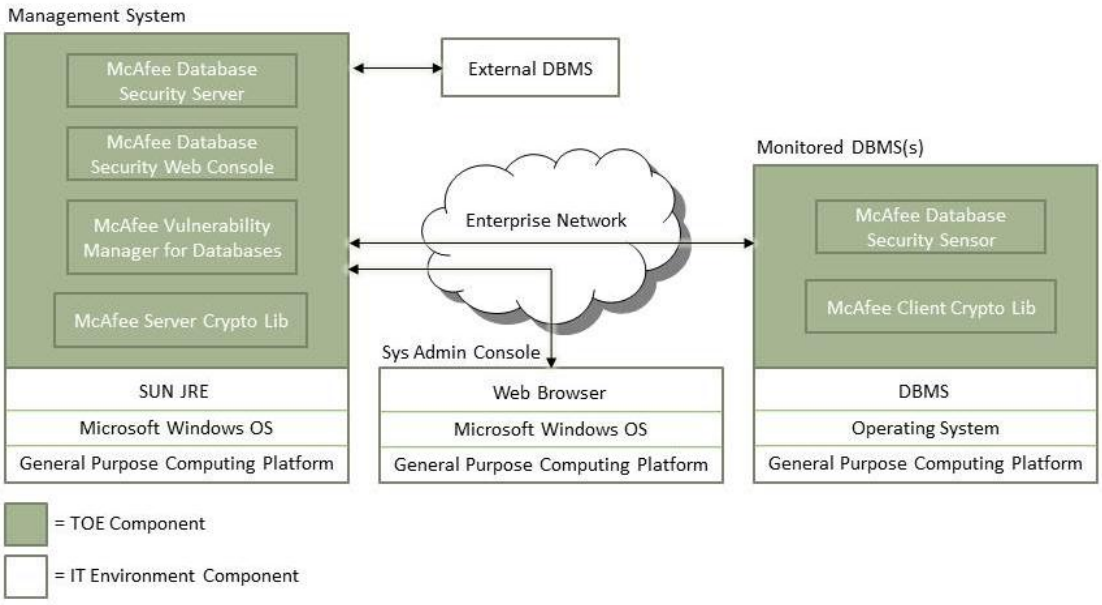

Figure 1 – TOE Boundary

The following specific configuration options apply to the evaluated configuration:

1. The IT Environment provides an external DBMS for alert storage, VA results, audit data and other system data.
2. The utilization of syslog servers, Windows event logs, XML API, email or Twitter accounts to send alerts and/or system messages has been excluded from the evaluated configuration.
3. Integration with McAfee ePO has been excluded from the evaluated configuration. All management is to be performed via the McAfee Database Security Web Console.
4. Updates to the TOE software are not permitted in the evaluated configuration.
5. Operating System (OS)-level vulnerability tests have been excluded from the evaluated configuration.[2]
6. Running the McAfee Database Security Server in cluster mode is not permitted in the evaluated configuration.
7. The use of predefined compliance rule sets have been excluded from the evaluation.[3]

1.7.2 Hardware and Software Supplied by the IT Environment

The TOE consists of a set of software applications. The hardware, operating systems and all third party support software (e.g., DBMS) on the systems on which the TOE executes are excluded from the TOE boundary.

[2] In addition to performing scans of a DBMS, the Vulnerability Manager also has the ability to perform credentialed scans of the host operating system (OS). When configuring a DBMS for vulnerability assessment, an OS user's credentials may be entered. However, this additional functionality has been omitted from the evaluation.

[3] The TOE supports compliance verification through the configuration of rules based on established international standards, including PCI-DSS, Sarbanes Oxley (SOX), SAS-70, GLBA and HIPAA. This functionality has been excluded from the evaluated configuration.

The platform on which the McAfee Database Security Server software is installed must be dedicated to functioning as the management system. The TOE requires the following hardware and software configuration on this platform.

COMPONENT	MINIMUM REQUIREMENTS
Memory	1 GB available RAM minimum 2 GB available RAM recommended
Free Disk Space	2 GB — Recommended minimum 30 MB - Recommended log directory space per monitored sensor
Operating System	Windows Server 2008 R2 Enterprise with Service Pack 1 Windows Server 2008 R2 Standard with Service Pack 1 Windows Server 2008 R2 Datacenter with Service Pack 1

Table 4 – Management System Component Requirements

McAfee Database Security Sensor executes on one or more DBMSs whose transactions are to be monitored. The supported platforms for these components are:

SUPPORTED OS (CHIPSET)	OS VERSION	DBMS
Windows (Intel x86 64-bit)	Windows Server 2008/2008 R2	MS-SQL 2005/2008

Table 5 – Supported DBMS Platforms

The minimum file system requirements for the DBMS platforms are specified in the following table:

COMPONENT	MINIMUM FILE SYSTEM REQUIREMENTS
Free Disk Space – DBMS	150 MB Minimum installation 400 MB Recommended

Table 6 – DBMS Platform Hardware Requirements

In addition, McAfee Vulnerability Manager for Databases will only execute VA scans & tests on the following supported DBMSs:

SUPPORTED DBMS PLATFORMS FOR VULNERABILITY ASSESSMENT
MS-SQL Server 2005, 2008 (on the platforms noted in Table 6)

Table 7 – Supported DBMS Platforms for Vulnerability Assessment Functionality

The management system is accessed from remote systems via the McAfee Database Security Web Console. The supported web browsers are Mozilla Firefox 10 and above, Microsoft Internet Explorer 8.0 and above, and Google Chrome (all versions). A minimum of 128 MB RAM is recommended.

1.7.3 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

TSF	DESCRIPTION

TSF	DESCRIPTION
DBMS Transaction Monitoring	The TOE monitors DBMS user and application activity by way of analysis of SQL statements interacting with the DBMS. Analysis of DBMS transactions is determined by a monitoring policy consisting of a set of rules (predefined and/or custom) which are configured to issue alerts and/or terminate suspicious activities. Alerts are sent from the McAfee Database Security Sensor to the McAfee Database Security Server for analysis where they are stored in the external database (provided by the IT environment) for subsequent analysis. Alerts and Reports are accessed via the McAfee Database Security Web Console.
DBMS Session Termination & User Quarantine	Prevention of intrusion, data theft, and other attacks on the DBMS is achieved in real-time through the termination of DBMS sessions. Predefined vPatch rules and/or custom rules can be created to detect and respond (by terminating the active session) to a range of attacks in accordance with organizational security policy. Manual termination of user DBMS sessions is also possible in response to an alert raised by the TOE. Administrators of the TOE also have the ability to quarantine users immediately following a termination event. A user can be placed in quarantine for a predefined number of minutes. While in quarantine, the user is unable to reconnect to the DBMSs for which the rule was triggered, unless the user is removed from the quarantine list by the Administrator.
Rule-based Policy Enforcement	Rule-based policies can be created for users, queries and/or DBMS objects. Rules define what types of statements and queries are allowed to run on the DBMS, what types are forbidden, and which types should be monitored. Incoming statements are compared to the rules enabled for the DBMS and action (allow, alert, or terminate) is taken based on the first rule that is matched. If a statement does not match any of the existing rules, the statement is allowed. The TOE provides enhanced DBMS security based on both predefined vPatch rules and custom rules. vPatch rules are included in the installation of the TOE and help prevent attacks against known vulnerabilities (such as SQL injection). In addition, custom rules can be defined to specify the level of monitoring and alerts, and further protect the DBMS(s) against potential threats. Rules can be applied to all DBMSs or to specific DBMSs and DBMS groups.

TSF	DESCRIPTION
Vulnerability Assessment	The TOE provides the capability of performing VA scans against monitored DBMSs to identify a wide range of risks and problems. VA scans are based on predefined and/or custom VA tests and are driven by compliance requirements and organizational policy. After running a VA scan, McAfee Vulnerability Manager for Databases provides detailed information about the scan findings via the Web Console. The administrator can then resolve identified findings in accordance with organizational policy and procedures.
Identification & Authentication	On the management system, the TOE requires users to identify and authenticate themselves before accessing the TOE software. User accounts must be defined within McAfee Database Security Server through the Web Console. No action can be initiated before proper identification and authentication (I&A). Each TOE user has security attributes associated with their user account that define the functionality the user is allowed to perform. On the management system and all managed DBMSs, I&A for local login to the operating system (i.e., via a local console) is performed by the local OS (IT Environment).
Management	The TOE's Management Security Function provides support functionality that enables users to configure and manage TOE components. Management of the TOE may be performed via the Web Console. Management privileges are defined per-user.
Audit	The TOE's Audit Security Function provides auditing of management actions performed by users (administrators). Authorized users may review the audit records via the Web Console.
Protected Data Transfer	The TOE consists of distributed components. Server to sensor communication relies upon cryptographic functionality provided by the TOE to protect the information exchanged from disclosure or modification.

Table 8 – Logical Boundary Descriptions

1.7.4 TOE Data

TOE data consists of both TSF data and user data (information). TSF data consists of authentication data, security attributes, and other generic configuration information. Security attributes enable the TOE to enforce the security policy. Authentication data enables the TOE to identify and authenticate users.

TSF Data	Description	AD	UA	GE
Alert	An alert is generated when the preconditions of an active rule have been met on a monitored DBMS.			✓

TSF Data	Description	AD	UA	GE
Alerts List	The list of all generated alerts including the alert level, DBMS, time and date the alert was generated, state information, resolution status, statement that triggered the alert, associated rules, and available actions.			✓
Application Map	A map of all applications running on monitored DBMSs, including the users running the applications.			✓
Data Retention	Parameters controlling the length of time alerts are saved in the database.			✓
DBMS Groups	Monitored DBMSs may be organized into groups for easier rule management.			✓
DBMS List	The list of all monitored DBMSs.			✓
Exceptions	Exceptions may be applied to the rule set or individual rules so that specific conditions do not trigger the rule.			✓
Permission	A privilege to perform a specific function.		✓	
Permission Set	A group of permissions that can be granted to any users by assigning it to those users' accounts.		✓	
Policy	A collection of rules that you create, configure, then enforce to ensure monitored DBMSs are protected from threats.			✓
Rule	Rules define what types of statements and queries are allowed to run on the DBMS, what types are forbidden, and which types should be monitored.			✓
Rule set	An organized set of rules that enforce the database security policy on monitored DBMSs. The rule set contains predefined, custom and vPatch rules.			✓
Security Dashboard	A wide range of statistical data regarding the status of alerts, DBMS monitoring, security updates, and rules that are refreshed at a user-configured interval.			✓
Tags	Tags are labels and are applied to specific rules. The tags can then be used to apply multiple rules to a DBMS, for ease of management.			✓
User Accounts	User name, role, authentication configuration, enabled status, and permission sets for each user authorized to access TOE functionality on the management system.	✓		
VA Results	The results of VA scans performed against monitored DBMSs.			✓
VA Scans	VA scans are based on one or more predefined and/or custom VA tests and are driven by compliance requirements and/or organizational policy.			✓
VA Tests	A test comprises specific checks that are to be performed against the monitored DBMSs.			✓

Table 9 – TOE Data (Legend: AD=Authentication data; UA=User attribute; GE=Generic Information)

1.8 Rationale for Non-bypassability and Separation of the TOE

The responsibility for non-bypassability and non-interference is split between the TOE and the IT Environment. TOE components are software only products and therefore the non-bypassability and

non-interference claims are dependent upon hardware and OS mechanisms. The TOE runs on top of the IT Environment supplied operating systems.

The TOE ensures that the security policy is applied and succeeds before further processing is permitted whenever a security relevant interface is invoked: the interfaces are well defined and ensure that the access restrictions are enforced. Non-security relevant interfaces do not interact with the security functionality of the TOE. The TOE depends upon OS mechanisms to protect TSF data such that it can only be accessed via the TOE. The system on which the McAfee Database Security Server, McAfee Database Security Web Console and McAfee Vulnerability Manager for Databases execute is dedicated to that purpose. The McAfee Database Security Sensor executes on the DBMSs; this component only performs transaction data collection and, with the exception of sending a terminate session command to the DBMS when a predefined rule condition has been met, do not enforce access control policies for users.

The TOE is implemented with well-defined interfaces that can be categorized as security relevant or non-security relevant. The TOE is implemented such that non-security relevant interfaces have no means of impacting the security functionality of the TOE. Unauthenticated users may not perform any actions within the TOE. The TOE ensures the access privileges of each user session are enforced.

The server hardware provides virtual memory and process separation, which the server OS utilizes to ensure that other (non-TOE) processes may not interfere with the TOE; all interactions are limited to the defined TOE interfaces. The OS and DBMS restrict access to TOE data in the database to prevent interference with the TOE via that mechanism.

The TOE consists of distributed components. Server to sensor communication relies upon cryptographic functionality provided by the TOE to protect the information exchanged from disclosure or modification.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 4 (September 2012) Part 2 extended and Part 3 conformant at Evaluation Assurance Level 2 and augmented by ALC_FLR.2 – Flaw Reporting Procedures.

2.2 Protection Profile Conformance Claim

The TOE does not claim conformance to a Protection Profile.

3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required.
- Any organizational security policy statements or rules with which the TOE must comply.
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

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

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.

Table 10 – Threats Addressed by the TOE

The following table identifies threats to the monitored DBMSs that may be indicative of vulnerabilities in or misuse of IT resources:

THREAT	DESCRIPTION
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

THREAT	DESCRIPTION
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on data acquired from the monitored DBMSs.
T.INADVE	Inadvertent activity and access may occur on a DBMS the TOE monitors.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on a DBMS the TOE monitors.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on a DBMS the TOE monitors.
T.SCNCFG	Improper security configuration settings may exist in the monitored DBMSs.
T.SCNMLC	Users could execute malicious code on a DBMS that the TOE monitors which causes modification of the DBMS protected data or undermines the DBMS security functions.
T.SCNVUL	Vulnerabilities may exist in the DBMS the TOE monitors.

Table 11 – Threats Addressed by the IT Environment

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. The following Organizational Security Policies apply to the TOE:

POLICY	DESCRIPTION
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to data received from data sources and appropriate response actions taken.
P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of a DBMS or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of DBMS assets must be collected.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

Table 12 – Organizational Security Policies

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION

ASSUMPTION	DESCRIPTION
A.ACCESS	The TOE has access to all the DBMS data it needs to perform its functions.
A.ASCOPE	The administrators will install as many TOE servers as necessary to support the number of sensors and DBMSs.
A.DATABASE	Access to the DBMS(s) managed by the TOE is restricted to authorized users.
A.DYNMIC	The TOE and its users are capable of managing an evolving threat landscape relative to the DBMSs monitored by the TOE.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
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.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.SECMGMT	Remote management communications between the TOE Web Console and the authorized administrator's web browser will be protected by HTTPS.
A.SSLDBMS	DBMS administrators will ensure that each managed and/or scanned DBMS has been configured to support Secure Sockets Layer (SSL) connections over its network interface.

Table 13 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ACCESS	The TOE must allow authorized users to access only authorized TOE functions and data.
O.AUDITS	The TOE must record audit records for data accesses and use of the TOE functions on the management system.
O.AUDIT_PROTECT	The TOE will provide the capability to protect audit information generated by the TOE.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.EXPORT	When any TOE component makes its data available to another TOE component, the TOE will ensure the confidentiality of the TOE data.
O.IDANLZ	The TOE must apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.IDSENS	The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of a monitored DBMS.
O.IDSCAN	The TOE must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of a DBMS.
O.INTEGR	The TOE must ensure the integrity of all TOE data.
O.OFLOWS	The TOE must appropriately handle potential TOE data storage overflows.
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.SD_PROTECTION	The TOE will provide the capability to protect TOE data.

Table 14 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.AUDIT_PROTECT	The IT Environment will provide the capability to protect audit information.
OE.AUDIT_REVIEW	The IT Environment will provide the capability for authorized administrators to review audit information generated by the TOE.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.

OBJECTIVE	DESCRIPTION
OE.DATABASE	Those responsible for the TOE must ensure that access to the managed DBMS(s) is restricted to authorized users only.
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 IT security.
OE.INTROP	The TOE is interoperable with the managed systems it monitors
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.PROTECT	The IT environment will protect the TOE and the DBMS(s) managed by the TOE from unauthorized access.
OE.SD_PROTECTION	The IT Environment will provide the capability to protect system data via mechanisms outside the TSC.
OE.STORAGE	The IT Environment will store TOE data in the external database and retrieve it when directed by the TOE.
OE.TIME	The IT Environment will provide reliable timestamps to the TOE

Table 15 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies (if applicable). The following table provides a high level mapping of coverage for each threat, assumption, and policy:

OBJECTIVE / THREAT / ASSUMPTION	O.IDSCAN	O.IDANLZ	O.EADMIN	O.ACCESS	O.IDAUTH	O.IDSENS	O.OFLOWS	O.INTEGR	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	O.AUDITS	O.AUDIT_PROTECT	O.EXPORT	O.RESPON	O.SD_PROTECTION	OE.TIME	OE.PROTECT	OE.SD_PROTECTION	OE.DATABASE	OE.AUDIT_PROTECT	OE.AUDIT_REVIEW	OE.STORAGE
A.ACCESS													✓												
A.ASCOPE													✓												
A.DATABASE																						✓			
A.DYNMIC												✓	✓												
A.LOCATE										✓															
A.MANAGE												✓													
A.NOEVIL									✓	✓	✓														
A.PROTCT										✓															
A.SECMGMT																					✓				
A.SSLDBMS																					✓				
P.ACCACT					✓									✓										✓	
P.ACCESS				✓	✓													✓			✓				
P.ANALYZ		✓																							
P.DETECT	✓					✓								✓					✓						
P.INTGTY								✓							✓								✓		✓
P.MANAGE			✓	✓	✓				✓		✓	✓													

OBJECTIVE / THREAT / ASSUMPTION	O.IDSCAN	O.IDANLZ	O.EADMIN	O.ACCESS	O.IDAUTH	O.IDSENS	O.OFLOWS	O.INTEGR	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	O.AUDITS	O.AUDIT_PROTECT	O.EXPORT	O.RESPON	O.SD_PROTECTION	OE.TIME	OE.PROTECT	OE.SD_PROTECTION	OE.DATABASE	OE.AUDIT_PROTECT	OE.AUDIT_REVIEW	OE.STORAGE
P.PROTCT							✓			✓						✓				✓					✓
T.COMDIS				✓	✓											✓				✓					
T.COMINT				✓	✓			✓												✓					
T.FACCNT														✓											
T.FALACT																	✓								
T.FALREC		✓																							
T.IMPCON			✓	✓	✓				✓																
T.INADVE						✓																			
T.LOSSOF				✓	✓			✓																	
T.MISACT						✓																			
T.MISUSE						✓																			
T.NOHALT	✓	✓		✓	✓																				
T.PRIVIL				✓	✓																				
T.SCNCFG	✓																								
T.SCNMLC	✓																								
T.SCNVUL	✓																								

Table 16 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

The following table provides detailed evidence of coverage for each threat, policy, and assumption:

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions. The OE.INTROP objective ensures the TOE has the needed access.
A.ASCOPE	The administrators will install as many TOE servers as necessary to support the number of sensors and DBMSs. The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.DATABASE	Access to the DBMS(s) managed by the TOE is restricted to authorized users. The OE.DATABASE objective ensures that access to the DBMS(s) managed by the TOE is granted to authorized users only.
A.DYNMIC	The TOE and its users are capable of managing an evolving threat landscape relative to the DBMSs monitored by the TOE. The OE.INTROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will be managed appropriately.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. The OE.PHYCAL provides for the physical protection of the TOE.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
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. The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. The OE.PHYCAL provides for the physical protection of the TOE hardware and software.
A.SECMGMT	Remote management communications between the TOE Web Console and the authorized administrator's web browser will be protected by HTTPS. The OE.SD_PROTECTION objective provides for the capability to protect system data via mechanisms outside the TSC. The user's web browser SSL implementation is a mechanism outside the TSC.
A.SSLDBMS	DBMS administrators will ensure that each managed and/or scanned DBMS has been configured to support Secure Sockets Layer (SSL) connections over its network interface. The OE.SD_PROTECTION objective provides for the capability to protect system data via mechanisms outside the TSC. The managed DBMS SSL implementation is a mechanism outside the TSC needed to protect system data during vulnerability scans.
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE. The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. The The OE.AUDIT_REVIEW objective provides the ability for administrators to review the audit records generated by the TOE so that accountability for administrator actions can be determined.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE function accesses via the web console. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.SD_PROTECTION and O.ACCESS objectives counter this threat for mechanisms inside the TSC via TOE protections of the system data trail and the database used to hold TOE data.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to data received from data sources and appropriate response actions taken. The O.IDANLZ objective addresses this policy by requiring the TOE to apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected. The O.AUDITS. O.IDSENS, and O.IDSCAN objectives address this policy by requiring collection of audit, sensor and policy scanner data. The OE.TIME objective supports this policy by providing a time stamp for insertion into the system data records.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification. The O.INTEGR objective ensures the protection of System data from modification. The O.AUDIT_PROTECT and OE.AUDIT_PROTECT objectives ensure the integrity of audit records in the database generated by the TOE using access mechanisms inside and outside the TSC respectively. The O.EXPORT objective requires the TOE to protect the data from unauthorized disclosure during transit. The OE.STORAGE objective requires the IT Environment to provide storage and retrieval mechanisms for System data for use by the TOE.
P.MANAGE	The TOE shall only be managed by authorized users. The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions. The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications. The OE.PROTECT objective supports the TOE protection from the IT Environment. The O.EXPORT objective requires the TOE to protect the data from unauthorized disclosure during transit. The OE.STORAGE objective requires the IT Environment to provide storage and retrieval mechanisms for System data for use by the TOE.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.EXPORT objective ensures that confidentiality of TOE data will be maintained. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no System data will be modified. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected. The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity. The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on data received from each data source. The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected. The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
T.INADVE	Inadvertent activity and access may occur on a DBMS the TOE monitors. The O.IDSENS objective addresses this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no System data will be deleted.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on a DBMS the TOE monitors. The O.IDSENS objective addresses this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on a DBMS the TOE monitors. The O.IDSENS objective addresses this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.IDSCAN and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. The O.IDAUTH objective provides for identification and authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
T.SCNCFG	Improper security configuration settings may exist in the DBMS the TOE monitors. The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change.
T.SCNMLC	Users could execute malicious code on a DBMS that the TOE monitors which causes modification of the DBMS protected data or undermines the DBMS System security functions. The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of malicious code.
T.SCNVUL	Vulnerabilities may exist in a DBMS the TOE monitors. The O.IDSCAN objective counters this threat by requiring a TOE that contains a Scanner, collect and store static configuration information that might be indicative of a vulnerability.

Table 17 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

5.1 IDS Class of SFRs

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

This class of requirements is copied from the IDS System PP to specifically address the data collected and analysed by an IDS scanner and analyser. The audit family 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 collecting, reviewing and managing the data.

5.1.1 IDS_SDC.1 System Data Collection

Management: IDS_SDC.1

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

a) Configuration of the events to be collected

Audit: IDS_SDC.1

There are no auditable events foreseen.

IDS_SDC.1 System Data Collection

Hierarchical to:	No other components
Dependencies:	No dependencies
IDS_SDC.1.1	The System shall be able to collect the following information from the targeted IT System resource(s): a) [selection: *Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration., accountability policy configuration, detected known vulnerabilities*]; and b) [assignment: *other specifically defined events*].
IDS_SDC.1.2	At a minimum, the System shall collect and record the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) The additional information specified in the Details column of the table below:

COMPONENT	EVENT	DETAILS
IDS_SDC.1	Startup and shutdown	None
IDS_SDC.1	Identification and authentication events	User identity, location, source address, destination address
IDS_SDC.1	Data accesses	Object IDS, requested access, source address, destination address
IDS_SDC.1	Service requests	Specific service, source address, destination address
IDS_SDC.1	Network traffic	Protocol, source address, destination address
IDS_SDC.1	Security configuration changes	Source address, destination address
IDS_SDC.1	Data introduction	Object IDS, location of object, source address, destination address
IDS_SDC.1	Startup and shutdown of audit functions	None
IDS_SDC.1	Detected malicious code	Location, identification of code
IDS_SDC.1	Access control configuration	Location, access settings
IDS_SDC.1	Service configuration	Service identification (name or port), interface, protocols
IDS_SDC.1	Authentication configuration	Account names for cracked passwords, account policy parameters
IDS_SDC.1	Accountability policy configuration	Accountability policy configuration parameters
IDS_SDC.1	Detected known vulnerabilities	Identification of the known vulnerability

Table 18 – System Data Collection Events and Details

Application Note: The rows in this table must be retained that correspond to the selections in IDS_SDC.1.1 when that operation is completed. If additional events are defined in the assignment in IDS_SDC.1.1, then corresponding rows should be added to the table for this element.

5.1.2 IDS_ANL.1 Analyzer Analysis

Management: IDS_ANL.1

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

a) Configuration of the analysis to be performed

Audit: IDS_ANL.1

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

a) Minimal: Enabling and disabling of any of the analysis mechanisms

IDS_ANL.1 Analyzer Analysis

Hierarchical to:	No other components
Dependencies:	No dependencies
IDS_ANL.1.1	The System shall perform the following analysis function(s) on all IDS data received: a) [selection: *statistical, signature, integrity*]; and b) [assignment: *other analytical functions*].
IDS_ANL.1.2	The System 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*]. (EXT)

5.1.3 IDS_RDR.1 Restricted Data Review (EXT)

Management: IDS_RDR.1

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: IDS_RDR.1

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

a) Basic: Attempts to read system data that are denied.

b) Detailed: Reading of information from the system data records.

IDS_RDR.1 Restricted Data Review

Hierarchical to:	No other components	
Dependencies:	IDS_SDC.1	System Data Collection
	IDS_ANL.1	Analyzer Analysis
IDS_RDR.1.1	The System shall provide [assignment: *authorized users*] with the capability to read [assignment: *list of System data*] from the System data.	
IDS_RDR.1.2	The System shall provide the System data in a manner suitable for the user to interpret the information.	
IDS_RDR.1.3	The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.	

5.1.4 IDS_RCT.1 – Analyzer React

Management: IDS_RCT.1

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

a) Configuration of the reaction operations to be performed

Audit: IDS_RCT.1

There are no auditable events foreseen.

IDS_RCT.1 Analyzer React

Hierarchical to:	No other components	
Dependencies:	IDS_SDC.1	System Data Collection
	IDS_ANL.1	Analyzer Analysis
IDS_RCT.1.1	The System shall send an alarm to [assignment: *specified location*] and take [assignment: *specified actions*] when an intrusion is detected.	

5.1.5 IDS_STG.1 Guarantee of System Data Availability

Management: IDS_STG.1

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

b) maintenance of the parameters that control the system data storage capability.

Audit: IDS_STG.1

There are no auditable events foreseen.

IDS_STG.1 Guarantee of System Data Availability

Hierarchical to:	No other components	
Dependencies:	IDS_SDC.1	System Data Collection
	IDS_ANL.1	Analyzer Analysis
IDS_STG.1.1	The System shall protect the stored System data from unauthorized deletion.	
IDS_ STG.1.2	The System shall protect the stored System data from modification.	
	Application Note: Authorized deletion of data is not considered a modification of System data in this context. This requirement applies to the actual content of the System data, which should be protected from any modifications.	
IDS_ STG.1.3	The System shall ensure that [assignment: *metric for saving System data*] System data will be maintained when the following conditions occur: [selection: *System data storage exhaustion, failure, attack*].	

5.1.6 IDS_STG.2 Prevention of System Data Loss

Management: IDS_STG.2

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

a) maintenance (deletion, modification, addition) of actions to be taken in case system data storage capacity has been reached.

Audit: IDS_STG.2

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

a) Basic: Actions taken if the storage capacity has been reached.

IDS_STG.2 Prevention of System data loss

Hierarchical to: No other components

Dependencies:	IDS_SDC.1	System Data Collection
	IDS_ANL.1	Analyzer Analysis

IDS_STG.2.1 The System shall [selection: *'ignore System data', 'prevent System data, except those taken by the authorized user with special rights', 'overwrite the oldest stored System data '*] and send an alarm if the storage capacity has been reached.

5.2 Extended Component – Audit Data Generation

For this evaluation the FAU_GEN.1 Security Functional Requirement in CC Part 2 has been extended to cover part of the TOE functionality that is not fully supported.

One additional component has been defined. This has been placed in an existing Family GEN: Audit Data Generation within the Class FAU: Security Audit. This choice has been made as the new component is a minor modification to the implementation of security auditing already defined in CC Part 2.

Specifically, the TOE does not generate an audit record of the following auditable event: startup and shutdown of the audit functions. An extended component FAU_GEN_EXT.1 has been added to remove the auditing of TOE startup and shutdown events. All other security requirements from FAU_GEN.1 remain identical.

5.2.1 FAU_GEN_EXT.1 Audit Data Generation (Extended)

Hierarchical to: No other components

Dependencies:	FPT_STM.1	Reliable Time Stamps

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

a) All auditable events for the [selection, choose one of*: minimum, basic, detailed, not specified*] level of audit; and

b) [assignment: *other specifically defined auditable events*].

FAU_GEN_EXT.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, [assignment: *other audit relevant information*].

6 Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, and those that were extended, all of which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN_EXT.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit Review
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG.3	Action in Case of Possible Audit Data Loss
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Distribution
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1	Cryptographic Operation
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UAU.1	Timing of Authentication
	FIA_UID.1	Timing of Identification
Security Management	FMT_MOF.1 (1)	Management of Security Functions Behavior
	FMT_MOF.1 (2)	Management of Security Functions Behavior
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF	FPT_ITT.1	TSF Data Transfer Protection
IDS Component Requirements	IDS_SDC.1	System Data Collection
	IDS_ANL.1	Analyzer Analysis
	IDS_RDR.1	Restricted Data Review
	IDS_RCT.1	Analyzer React
	IDS_STG.1	Guarantee of System Data Availability
	IDS_STG.2	Prevention of System Data Loss

Table 19 – TOE Functional Components

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN_EXT.1 Audit Data Generation (Extended)

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

a) All auditable events for the not specified level of audit; and

b) *The events identified in the following table*

FAU_GEN_EXT.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, 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, *the information detailed in the following table*.

Application Note: The auditable events for the respective level of auditing are included in the following table:

COMPONENT	EVENT	DETAILS
FAU_SAR.2	Note: Unsuccessful attempts to read information from the audit records do not occur because the TOE does not present that capability to users that are not authorized to read the audit records.	None
FAU_STG.3	Note: Old audit records (alerts) are archived when the audit trail exceeds the archive settings limits for the audit trail.	None
FIA_ATD.1	All changes to TSF data result in an audit record being generated.	None
FIA_UAU.1	All use of the user authentication mechanism	User identity, location
FIA_UID.1	All use of the user identification mechanism	User identity, location
FMT_MOF.1 (1)	All modifications in the behavior of the functions of the TSF	None
FMT_MOF.1 (2)	All modifications in the behavior of the functions of the TSF	None
FMT_MTD.1	All modifications to the values of TSF data	None
FMT_SMF.1	Use of the management functions	User identity, function used
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity
IDS_ANL.1	None (the analysis function is always enabled)	None
IDS_RDR.1	None (the user is not given the option of accessing unauthorized system data)	None

COMPONENT	EVENT	DETAILS
IDS_STG.2	Note: A system message is generated indicating when older audit records (alerts) are archived and then overwritten by newer audit records. This condition occurs once the predetermined number of alerts has been reached in the external database.	None

Table 20 – Audit Events and Details

6.1.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *Admin, McAfee Database Security Operator and Read Only users* with the capability to read *all 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.

6.1.1.4 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.5 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorized modifications to the audit records in the audit trail.

6.1.1.6 FAU_STG.3 Action in Case of Possible Audit Data Loss

FAU_STG.3.1 The TSF shall archive and remove the oldest Alerts from the external database if the audit trail exceeds the archive settings for the audit trail.

Application Note: This requirement only applies to the archival of the alerts.

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*ANSI X9.31*] and specified cryptographic key sizes [*128-, 192-, or 256-bit AES key and 168-bit TDES key*] that meet the following: [*FIPS 197 for AES and FIPS 46-3 for TDES*].

6.1.2.2 FCS_CKM.2 Cryptographic Key Distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [*RSA*] that meets the following: [*TLS v1.2 specification RFC 5246*].

6.1.2.3 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*Federal Information Processing Standard 140 requirements for key zeroization*].

6.1.2.4 FCS_COP.1 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform [*the operations described below*] in accordance with a specified cryptographic algorithm [*multiple algorithms in the modes of operation described below*] and cryptographic key sizes [*multiple key sizes described below*] that meet the following: [*multiple standards described below*].

Table 21 – Cryptographic Operations

OPERATION	ALGORITHM (MODE)	KEY SIZE IN BITS	CAVP CERTIFICATE	STANDARDS
Encryption and Decryption	AES	128, 256	1544 / 1547	FIPS 197
	TDES	168	1014 / 1017	FIPS 46-3
Hashing	SHA-1	160	1369 / 1374	FIPS 180-3
Digital Signatures	DSA	Modulus Size: 1024, 2048	476 / 479	FIPS 186-3
	RSA	Modulus Size: 1024, 2048	747 / 752	ANSI X9.31 PKCS #1 v1.5 RSASSA-PSS
Random Number Generation	ANSI X9.31	Not Applicable	832 / 836	ANSI X9.31
Key Distribution	RSA	Modulus Size: 1024, 2048	747 / 752	ANSI X9.31 PKCS #1 v1.5 RSASSA-PSS

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) Username;

b) Status (active or inactive);

c) Password;

d) Assigned Permissions; and

e) *Assigned Role.*

6.1.3.2 FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow *no actions* on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.3 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow *no actions* on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MOF.1 Management of Security Functions Behavior (1)

FMT_MOF.1.1 (1) The TSF shall restrict the ability to modify the behavior of the functions of *system data collection and reaction* to *Admin and Policy Creator*.

Application Note: System data collection and reaction in this context refers to the collection and reaction functions performed by the Sensor. Vulnerability assessment management functions are performed by the Server and are covered by FMT_MOF.1 (2).

6.1.4.2 FMT_MOF.1 Management of Security Functions Behavior (2)

FMT_MOF.1.1 (2) The TSF shall restrict the ability to modify the behavior of the functions of *vulnerability assessment management* to *Admin*.

6.1.4.3 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to change default, query, modify, delete the *TSF data identified in the following table to a user with the permissions identified in the following table* to *McAfee Database Security Operator, Policy Creator, Read Only or Read Only Alerts authorized roles.*

*Application Note: The TOE has several user roles with differing permissions to access TSF data. The Admin role has full permissions to change default, query, modify and delete all TSF data. The table below provides a mapping of user roles to the operations permitted on the TSF data. Authorized roles have been abbreviated to **SO** = McAfee Database Security Operator, **PC** = Policy Creator, **RO** = Read Only and **RA** = Read Only Alerts. Note the Admin role is not shown in the table below to enhance clarity of the other user roles.*

Table 22 – TSF Data Access Permissions for Authorized Users

TSF Data	Change Default	Query	Modify	Delete
Alert	SO	SO RO RA	SO	SO
Alerts List	SO	SO RO RA	SO	SO
Application Map	SO PC	SO PC RO	SO PC	SO PC
Data Retention	SO PC	SO PC RO	SO PC	SO PC
DBMS Groups	PC	SO PC RO	PC	PC
DBMS List	PC	SO PC RO	PC	PC
Exceptions	PC	SO PC RO	PC	PC
Permission	SO	SO RO	SO	SO
Permission Set	SO	SO RO	SO	SO
Policy	PC	PO PC RO	PC	PC
Rule	PC	SO PC RO	PC	PC
Rule set	PC	SO PC RO	PC	PC
Security Dashboard	RA RO SO	SO RO RA	SO RO RA	N/A
Tags	PC	SO PC RO	PC	PC
User Accounts	SO	SO RO	SO	SO
VA Results		RO		
VA Scans		RO		
VA Tests		RO		

6.1.4.4 FMT_SMF.1 Specification of Management Functions

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

a) User Account management,

b) Permission Set management,

c) Alert Archive management,

d) History List management,

e) Rule management,

f) Alert management,

g) Sensor management,

h) Security Dashboard management, and

i) VA management

6.1.4.5 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles: *Admin, Read Only, McAfee Database Security Operator, Policy Creator, and Read Only Alerts*.

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

Application Note: The Admin role is used to install and configure the TOE. Once the TOE is in operation separation of duties is enforced through only using the following roles: Read Only, McAfee Database Security Operator, Policy Creator, and Read Only Alerts.

Application Note: Read Only users can view all screens and settings, but cannot make changes to the TSF data or settings. McAfee Database Security Operators can perform operations in the system, but cannot change the security policy and related objects. Policy Creators can create and edit rules, and configure other system components, but cannot view alerts. Read Only Alert users have read-only access to the Security Dashboard and the Alerts list. Admin users can view, edit and delete all settings.

6.1.5 Protection of the TSF (FPT)

6.1.5.1 FPT_ITT.1 TSF Data Transfer Protection

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure, modification when it is transmitted between separate parts of the TOE.

Application Note: Transmission of TSF data between the sensor and server components is encrypted.

6.1.6 IDS Component Requirements (IDS)

6.1.6.1 IDS_SDC.1 System Data Collection

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) Identification and authentication events, data accesses, security configuration changes, data introduction, detected malicious code, access control configuration, authentication configuration, detected known vulnerabilities; and

b) no other events.

IDS_SDC.1.2 At a minimum, the System shall collect and record the following information:

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

b) The additional information specified in the *Details* column **of the table**

below.

COMPONENT	EVENT	DETAILS
IDS_SDC.1	Identification and authentication events	User identity, location, source address, destination address
IDS_SDC.1	Data accesses	Object IDS, requested access, source address, destination address
IDS_SDC.1	Security configuration changes	Source address, destination address
IDS_SDC.1	Data introduction	Object IDS, location of object, source address, destination address
IDS_SDC.1	Detected malicious code	Location, identification of code
IDS_SDC.1	Access control configuration	Location, access settings
IDS_SDC.1	Authentication configuration	Account names for cracked passwords, account policy parameters
IDS_SDC.1	Detected known vulnerabilities	Identification of the known vulnerability

Table 23 – System Data Collection Events and Details

6.1.6.2 IDS_ANL.1 Analyzer analysis

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all system data received:

a) Statistical, signature*;* and

b) No other functions.

Application Note: The TOE can be configured to perform statistical analysis by identifying deviations from normal patterns of behaviour (such as abnormal usage) through the definition of one or more rules. Signature analysis is provided primarily through vPatch rules which can prevent attacks against known vulnerabilities. Custom rules can also be created to provide either statistical or signature analysis.

IDS_ANL.1.2 The System 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) DBMS user, OS user, SQL statement (that triggered the alert), name of the affected DBMS, IP address of the user (if applicable), application that created the SQL statement, hostname of the user (if applicable), and alert ID.

6.1.6.3 IDS_RCT.1 Analyzer React

IDS_RCT.1.1 The System shall send an alarm to *console* and take *no further action or terminate the session and/or quarantine the user* when an intrusion is detected.

6.1.6.4 IDS_RDR.1 Restricted Data Review (EXT)

IDS_RDR.1.1 The System shall provide *a user with the role Admin, Read Only, McAfee Database Security Operator or Read Only Alerts* with the capability to read *alerts* from the System data.

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

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

6.1.6.5 IDS_STG.1 Guarantee of System Data Availability

IDS_STG.1.1 The System shall protect the stored System data from unauthorized deletion.

IDS_ STG.1.2 The System shall protect the stored System data from modification.

Application Note: Authorised deletion of data is not considered a modification of System data in this context. This requirement applies to the actual content of the System data, which should be protected from any modifications.

IDS_ STG.1.3 The System shall ensure that *(to the limits of the storage space for the configured data retention period) the most recent* System data will be maintained when the following conditions occur: System data storage exhaustion.

6.1.6.6 IDS_STG.2 Prevention of System data loss

IDS_STG.2.1 The System shall overwrite the oldest stored System data and send an alarm if the storage capacity has been reached.

Application Note: The overwriting of system data in this context refers to the overwriting of the oldest alerts. In accordance with FAU_STG.3, alerts are archived when a pre-determined number of alerts have been reached. Archiving the alerts will cause the oldest alerts to be overwritten with newer alerts as they populate the database. When an archive action occurs, an "Archiving Alerts" message (alarm) is displayed at the top of the alerts list. Status of the archived alerts can also be verified by checking the System->Archives->Archive History tab in the Web Console.

6.2 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2) augmented by ALC_FLR.2. The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle 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
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing – Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 24 – Security Assurance Requirements at EAL2

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.

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_GEN_EXT.1	No other components	FPT_STM.1	Satisfied by OE.TIME in the environment
FAU_GEN.2	No other components	FAU_GEN.1, FIA_UID.1	Satisfied by FAU_GEN_EXT.1 Satisfied
FAU_SAR.1	No other components	FAU_GEN.1	Satisfied by FAU_GEN_EXT.1
FAU_SAR.2	No other components	FAU_SAR.1	Satisfied
FAU_STG.1	No other components	FAU_GEN.1	Satisfied by FAU_GEN_EXT.1
FAU_STG.3	No other components	FAU_STG.1	Satisfied
FCS_CKM.1	No other components	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Satisfied

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FCS_CKM.2	No other components	FDP_ITC.1 or FDP_IDC.2 or FCS_CKM.1 FCS_CKM.4	Satisfied
FCS_CKM.4	No other components	FDP_ITC.1 or FDP_IDC.2 or FCS_CKM.1	Satisfied
FCS_COP.1	No other components	FDP_ITC.1 or FDP_IDC.2 or FCS_CKM.1 FCS_CKM.4	Satisfied
FIA_ATD.1	No other components	None	n/a
FIA_UAU.1	No other components	FIA_UID.1	Satisfied
FIA_UID.1	No other components	None	n/a
FMT_MOF.1	No other components	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
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
FPT_ITT.1	No other components	None	n/a
IDS_SDC.1	No other components	None	None
IDS_ANL.1	No other components	None	None
IDS_RCT.1	No other components	IDS_SDC.1, IDS_ANL.1	Satisfied Satisfied
IDS_RDR.1	No other components	IDS_SDC.1, IDS_ANL.1	Satisfied Satisfied
IDS_STG.1	No other components	IDS_SDC.1, IDS_ANL.1	Satisfied Satisfied
IDS_STG.2	No other components	IDS_SDC.1, IDS_ANL.1	Satisfied Satisfied

Table 25 – TOE SFR Dependency Rationale

6.4 Security Requirements Rationale

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

6.4.1 Security Functional Requirements for the TOE

The following table provides a high level mapping of coverage for each security objective:

SFR \ OBJECTIVE	O.ACCESS	O.AUDITS	O.AUDIT_PROTECT	O.EADMIN	O.IDANLZ	O.IDAUTH	O.IDSCAN	O.IDSENS	O.EXPORT	O.INTEGR	O.OFLOWS	O.RESPON	O.SD_PROTECTION
FAU_GEN_EXT.1		✓											
FAU_GEN.2		✓											
FAU_SAR.1	✓			✓									
FAU_SAR.2	✓					✓							
FAU_STG.1		✓	✓										
FAU_STG.3		✓									✓		
FCS_CKM.1									✓	✓			
FCS_CKM.2									✓	✓			
FCS_CKM.4									✓	✓			
FCS_COP.1									✓	✓			
FIA_ATD.1						✓							
FIA_UAU.1	✓					✓							
FIA_UID.1	✓					✓							
FMT_MOF.1 (1)	✓					✓							✓
FMT_MOF.1 (2)	✓					✓							✓
FMT_MTD.1	✓			✓		✓				✓			✓
FMT_SMF.1	✓			✓									
FMT_SMR.1	✓			✓		✓							
FPT_ITT.1									✓	✓			
IDS_SDC.1							✓	✓					
IDS_ANL.1					✓								
IDS_RCT.1												✓	
IDS_RDR.1	✓			✓		✓							
IDS_STG.1	✓					✓				✓			✓
IDS_STG.2											✓		

Table 26 – Mapping of TOE SFRs to Security Objectives

The following table provides detailed evidence of coverage for each security objective:

OBJECTIVE	RATIONALE

OBJECTIVE	RATIONALE
O.ACCESS	The TOE must allow authorized users to access only authorized TOE functions and data. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1]. Users authorized to access the TOE are determined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1(1), FMT_MOF.1(2)]. The permitted access to TOE data by the roles and permissions is defined [FMT_MTD.1, FMT_SMF.1, FMT_SMR.1]. The audit log records may only be viewed by authorized users (FAU_SAR.1, FAU_SAR.2].
O.AUDITS	The TOE must record audit records for data accesses and use of the TOE functions on the management system. Security-relevant events must be defined and auditable for the TOE [FAU_GEN_EXT.1]. The user associated with the events must be recorded [FAU_GEN.2]. The TOE must provide the capability to select which security-relevant events to audit [FAU.SEL.1]. In the event of audit event storage reaches a predefined limit, the oldest events (alerts) are archived and notification of the situation is provided [FAU_STG.3]. The TOE does not provide any mechanism for users to modify or delete audit records other than via configuration of the data retention timeframe, and that functionality is limited to administrators [FAU_STG.1].
O.AUDIT_PROTECT	The TOE will provide the capability to protect audit information generated by the TOE. The TOE is required to protect the stored audit records from unauthorized deletion or modification [FAU_STG.1].
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data. The TOE must provide the ability to review and manage the audit trail of the System [FAU_SAR.1]. The System must provide the ability for authorized administrators to view all System data collected and produced [IDS_RDR.1]. The functions and roles required for effective management are defined [FMT_SMF.1, FMT_SMR.1], and the specific access privileges for the roles and permissions is enforced [FMT_MTD.1].
O.IDANLZ	The TOE must apply analytical processes and information to derive conclusions about intrusions (past, present, or future). The TOE is required to perform intrusion analysis and generate conclusions [IDS_ANL.1].

OBJECTIVE	RATIONALE
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. Security attributes of subjects used to enforce the security policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1(1), FMT_MOF.1(2)]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1].
O.IDSCAN	The TOE must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of a DBMS. The TOE is required to collect and store static configuration information of a DBMS. The type of configuration information collected is defined [IDS_SDC.1].
O.IDSENS	The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of a monitored DBMS. The TOE is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of a monitored DBMS. These events are defined [IDS_SDC.1].
O.EXPORT	When any TOE component makes its data available to another TOE component, the TOE will ensure the confidentiality of the TOE data. The TOE must protect TSF data from disclosure, modification when it is transmitted between separate parts of the TOE [FPT_ITT.1]. The TOE ensures the confidentiality of system data through the implementation of encrypted communications [FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1] between TOE components.
O.INTEGR	The TOE must ensure the integrity of all TOE data. Only authorized administrators of the System may query or add System data [FMT_MTD.1]. The TOE is required to protect all system data from unauthorized modification or deletion [IDS_STG.1]. The TOE must protect TSF data from modification when it is transmitted between separate parts of the TOE [FPT_ITT.1]. The TOE ensures the integrity of system data through the implementation of encrypted communications [FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1] between TOE components.

OBJECTIVE	RATIONALE
O.OFLOWS	The TOE must appropriately handle potential TOE data storage overflows. The TOE must take action in case of possible loss of audit data (alerts) in the event the audit trail exceeds a predefined limit [FAU_STG.3]. The System must prevent the loss of system data in the event its trail is full [IDS_STG.2].
O.RESPON	The TOE must respond appropriately to analytical conclusions. The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT.1].
O.SD_PROTECTION	The TOE will provide the capability to protect TOE data. The TOE is required to protect the System data from unauthorized deletion or modification [IDS_STG.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1(1), FMT_MOF.1(2)]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1].

Table 27 – Rationale for Mapping of TOE SFRs to Objectives

6.4.2 Security Assurance Requirements

This section identifies the Configuration Management, Delivery/Operation, Development, Test, and Guidance measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Architecture Description: McAfee Database Security 4.4.3
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: McAfee Database Security 4.4.3
ADV_TDS.1: Basic Design	Basic Design: McAfee Database Security 4.4.3
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: McAfee Database Security 4.4.3
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: McAfee Database Security 4.4.3
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: McAfee Database Security 4.4.3
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: McAfee Database Security 4.4.3
ALC_DEL.1: Delivery Procedures	Delivery Procedures: McAfee Database Security 4.4.3
ATE_COV.1: Evidence of Coverage	Security Testing: McAfee Database Security 4.4.3
ATE_FUN.1: Functional Testing	Security Testing: McAfee Database Security 4.4.3
ATE_IND.2: Independent Testing – Sample	Security Testing: McAfee Database Security 4.4.3

Table 28 – Security Assurance Measures

6.4.2.1 Rationale for TOE Assurance Requirements Selection

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

1. Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.
2. The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.
3. Consistent with current best practice for tracking and fixing flaws as well as providing fixes to customers.

6.5 TOE Summary Specification Rationale

This section demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs.

The following tables provide a mapping between the TOE's Security Functions and the SFRs and the rationale.

SFR \ TSF	DBMS Transaction Monitoring	DBMS Session Termination & User Quarantine	Rule-based Policy Enforcement	Vulnerability Assessment	Identification & Authentication	Management	Audit	Protected System Data Transfer
FAU_GEN_EXT.1							✓	
FAU_GEN.2							✓	
FAU_SAR.1							✓	
FAU_SAR.2							✓	
FAU_STG.1							✓	
FAU_STG.3							✓	
FCS_CKM.1								✓
FCS_CKM.2								✓
FCS_CKM.4								✓
FCS_COP.1								✓
FIA_ATD.1						✓		
FIA_UAU.1					✓			
FIA_UID.1					✓			

SFR \ TSF	DBMS Transaction Monitoring	DBMS Session Termination & User Quarantine	Rule-based Policy Enforcement	Vulnerability Assessment	Identification & Authentication	Management	Audit	Protected System Data Transfer
FMT_MOF.1 (1)						✓		
FMT_MOF.1 (2)						✓		
FMT_MTD.1						✓		
FMT_SMF.1						✓		
FMT_SMR.1						✓		
FPT_ITT.1								✓
IDS_SDC.1	✓		✓					
IDS_ANL.1	✓			✓				
IDS_RCT.1		✓	✓					
IDS_RDR.1	✓					✓		
IDS_STG.1	✓					✓	✓	
IDS_STG.2	✓					✓	✓	

Table 29 – SFR to TOE Security Functions Mapping

SFR	SF AND RATIONALE
FAU_GEN_EXT.1	**Audit –** User actions are audited according to the events specified in the table with the SFR.
FAU_GEN.2	**Audit –** The audit log records include the associated user name when applicable.
FAU_SAR.1	**Audit –** Audit log records are displayed in a human readable table form from queries generated by authorized users.
FAU_SAR.2	**Audit –** Only authorized users have permission to query audit log records.
FAU_STG.1	**Audit –** The only mechanism provided by the TOE to cause audit records to be deleted is configuration of the data retention timeframe, which is restricted to administrators. The TOE does not provide any mechanism for users to modify audit records.
FAU_STG.3	**Audit –** If the predefined number of alerts has been reached, the TOE will archive the oldest events (alerts) in the external database.
FCS_CKM.1	**Protected System Data Transfer** – The TOE provides secure communications between the server and monitored DBMS sensors, in part, through the generation of cryptographic keys used to establish encrypted sessions for the safe passage of TSF data.
FCS_CKM.2	**Protected System Data Transfer** – The TOE provides secure communications between the server and monitored DBMS sensors, in part, through the secure distribution of cryptographic keys used to establish encrypted sessions for the safe passage of TSF data.

SFR	SF AND RATIONALE
FCS_CKM.4	**Protected System Data Transfer** – The TOE provides secure communications between the server and monitored DBMS sensors, in part, through the secure destruction of cryptographic keys used to establish encrypted sessions for the safe passage of TSF data.
FCS_COP.1	**Protected System Data Transfer** – The TOE provides secure communications between the server and monitored DBMS sensors which allow the safe passage of TSF data between TOE components.
FIA_ATD.1	**Management** – User security attributes are associated with the user account via User Account management.
FIA_UAU.1	**Identification & Authentication** - The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TSC. No action can be initiated before proper identification and authentication.
FIA_UID.1	**Identification & Authentication** - The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TSC. No action can be initiated before proper identification and authentication.
FMT_MOF.1 (1)	**Management** - The ability to modify the behaviour of the functions of System data collection and reaction are restricted to the Admin and Policy Creator roles.
FMT_MOF.1 (2)	**Management** - The ability to modify the behaviour of the functions of vulnerability assessment management are restricted to the Admin role.
FMT_MTD.1	**Management** – The user role (Admin, Read Only, Read Only Alerts, McAfee Database Security Operator and Policy Creator) and associated user permissions determine the access privileges of the user to TOE data.
FMT_SMF.1	**Management** – The management functions that must be provided for effective management of the TOE are defined and described.
FMT_SMR.1	**Management** – The TOE provides the roles specified in the SFR.
FPT_ITT.1	**Protected System Data Transfer** – The TOE encrypts all communication sessions between the sensors and server protecting TSF data from unauthorized disclosure and unauthorized modification.
IDS_SDC.1	**DBMS Transaction Monitoring/Rule-based Policy Enforcement** – The TOE monitors specified DBMSs in order to protect each system from internal and external threats, which includes vulnerability detection as enforced by vPatch and custom rules. System alerts are stored in the external database.
IDS_ANL.1	**DBMS Transaction Monitoring/Vulnerability Assessment** – The TOE analyses the results of the alerts and VA results performed to indicate vulnerabilities on each monitored DBMS. Vulnerability results and alert data are stored in the external database.

SFR	SF AND RATIONALE
IDS_RCT.1	**DBMS Session Termination & User Quarantine/Rule-based Policy Enforcement** – The TOE can create rules whereby if they trigger the TOE will react by terminating the session and (optionally) also quarantine the user for a predefined period of time.
IDS_RDR.1	**DBMS Transaction Monitoring/Management** – The TOE provides the ability for authorized administrators to retrieve reports (alerts) from the external database that describe the results from the monitoring, which includes detected vulnerabilities.
IDS_STG.1	**DBMS Transaction Monitoring/Management/Audit** – The TOE protects the alert information from unauthorized deletion and modification via interfaces within the TSC because no mechanism exists for modification.
IDS_STG.2	**DBMS Transaction Monitoring/Management/Audit** – If the storage space in the external database is exhausted (by reaching the predetermined number of alerts threshold), the oldest data is archived and then overwritten by the newer data.

Table 30 – SFR to TSF Rationale

7 TOE Summary Specification

7.1 DBMS Transaction Monitoring

The TOE monitors DBMS user and application activity by way of analysis of SQL statements interacting with the DBMS. Analysis of DBMS transactions is determined by a monitoring policy consisting of a set of rules (predefined and/or custom) which are configured to issue alerts and/or terminate suspicious activities. Rules are provided by the Rule-based Policy Enforcement TSF.

Alerts are sent from the McAfee Database Security Sensor to the McAfee Database Security Server for analysis where they are stored in the external database (provided by the IT Environment) for subsequent analysis. Alerts and Reports are accessed via the McAfee Database Security Web Console.

7.1.1 Alerts

Alerts are the primary method of communicating abnormal or suspicious activity to the Administrator. Alerts are displayed to the Administrator via the alerts list which consists of the information needed by the Administrator to perform review and take any further action if necessary. Each alert contains the following information and/or available actions:

- Level: alert severity levels may be one of low, medium, high, notice or informational.
- DBMS: the name of the DBMS for which the alert was generated.
- Time: data and time the alert was generated.
- User: both the OS and/or DBMS user is identified (if available). IP address is and the user hostname
- State: compares previous results to current results. Values are new, old or no change.
- Duplicate alerts amount: a count of repeated alerts if submitted frequently within the same session.
- Resolution: describes the current state of the alert. Examples are unresolved, resolved, false alarm, session terminated.
- Statement: the requested operation (original SQL statement) that triggered the alert.
- Application: the application that created the SQL statement.
- Rules: the names(s) of the rule(s) that generated the alert.
- Actions: the actions that can be performed on the alert. Administrators may choose to do one of the following:

- **Create a new rule** based on the alert parameters to monitor future occurrences.
- **Resolve alert** allows the Administrator to change the status of the alert (after review) to either resolved or false alarm.
- **Create a rule based on alert** can be done to create an exception to prevent repeated occurrence of false positives.
- **Trust session** if the Administrator decides the alert does not warrant further monitoring, all future alerts for that particular session can be ignored. Sessions are identified by the system according to the DBMS session ID and an internal ID.
- **Terminate session** if the Administrator deems the alert to be in violation of the organization's security policy.
- **Excessive behavior** indicates to the Administrator that a rule has triggered an alert more than once.

Administrators may create filters to make it easier to sort through the alert list. Criteria may also be defined to change how alerts are displayed in the alerts list.

7.1.2 Security Dashboard

The monitoring function of the TOE is performed via the console using the Security Dashboard. The Dashboard displays a wide range of statistical data regarding the status of alerts. For easier management Administrators can set the time interval of the data to be displayed by selecting the relevant time period e.g. last 10 min, last hour, last week, etc.

The Dashboard displays the following types of statistical data for the selected timeframe:

- Unresolved Alerts: Indicates the distribution of unresolved alerts in all monitored DBMSs according to severity (High, Medium, Low).
- Alerts per DBMSs: Indicates the distribution of alerts per DBMS according to severity (High, Medium, Low) in the selected system or the Administrator selected DBMSs.
- Sensors Status: Indicates the distribution of sensors according to status – Down, Pending, or Up. (Pending sensors are sensors that have not been approved by the administrator.)
- DBMS Status: Indicates the distribution of DBMSs according to their monitoring status – Monitored, Partly Monitored, or Unmonitored. (Partly monitored DBMSs are clustered DBMSs where only some members are currently monitored.)
- Alerts Summary: Indicates the distribution of alerts (all types) according to severity (High, Medium, Low) across the selected time period.

- Quarantine List: Lists the elements currently in quarantine, including the start time, the DBMS, and the rule that triggered the quarantine.
- Installed Security Updates: Lists the installed security updates, including version number, date installed, and the person responsible for their installation.
- Available Security Updates: Lists the available security updates, including version number, when published, and a brief description (if available). Please note to comply with the evaluated version the download of updates is not allowed.
- Most Active vPatch: Lists the most active vPatch rules in the system, including the rule name, the DBMS on which the rule is installed, and the number of alerts (based on the time selected at the top of the screen).
- Most Active Custom Rules: Lists the most active custom rules in the system, including the rule name, the DBMS on which the rule is installed, and the number of alerts (based on the time selected at the top of the screen).

7.2 DBMS Session Termination & User Quarantine

Prevention of intrusion, data theft, and other attacks on the DBMS is achieved in real-time through the termination of DBMS sessions via the Security Dashboard. Predefined vPatch rules and/or custom rules can be created to detect and respond (by terminating the active session) to a range of attacks in accordance with organizational security policy. Manual termination of user DBMS sessions is also possible in response to an alert raised by the TOE.

Administrators of the TOE also have the ability to quarantine users immediately following a termination event. A user can be placed in quarantine for a predefined number of minutes. While in quarantine, the user is unable to reconnect to the DBMSs for which the rule was triggered, unless the user is removed from the quarantine list by the Administrator.

7.3 Rule-based Policy Enforcement

DBMSs are manipulated by SQL statements and queries on an ongoing basis. The monitoring policy for a DBMS comprises the various rules that are enabled and applied on that DBMS. Rule-based policies can be created for users, queries and/or DBMS objects. Rules define what types of statements and queries are allowed to run on the DBMS, what types are forbidden, and which types should be monitored. Incoming statements are compared to the rules enabled for the DBMS and action (allow, alert, or terminate) is taken based on the first rule that is matched. If a statement does not match any of the existing rules, the statement is allowed.

The TOE provides enhanced DBMS security based on both predefined vPatch rules and custom rules. vPatch rules are included in the installation of the TOE and help prevent attacks against known

vulnerabilities (such as SQL injection). vPatch rules are enabled with a valid subscription (license) to Virtual Patching for Databases. Once enabled, the user (Policy Creator) has access to a large number of predefined rules (i.e. the vPatch rules) that are used by the sensors to monitor the DBMS for the existence of many types of known vulnerabilities. In addition, custom rules can be defined to specify the level of monitoring and alerts, and further protect the DBMS(s) against potential threats. For example, custom rules can be used to limit access to specific tables in the DBMS, or to limit access to the DBMS by specific users or at specific times of day.

Rules are defined and/or enabled per one or more DBMSs. Rules for each DBMS are managed in the various tabs of the DBMS Properties page. vPatch rules are listed in the vPatch Rules tab of the DBMS properties page. Custom rules are listed in the Custom Rules tab of the DBMS properties page. Incoming statements are checked against the vPatch list before they are checked against the Custom Rules list because the vPatch rules deal mostly with known attacks and therefore should not be overruled by custom rules. Administrators can disable all of the vPatch rules or specific rules if the need arises, for example, in case of false positives where exceptions are unable to resolve the issue.

7.3.1 Rule Parameters

Rules are the mechanism by which the TOE protects the DBMS. Each rule contains the following parameters:

- Enabled/Disabled: An icon indicating the status of the rule, enabled or disabled.
- No.: The ID number of the rule.
- Name: The name of the rule.
- Rule: The comparator statements (Identifiers, Operators & Literals) that serve as the criteria for matching the rule against the incoming or outgoing SQL statement.
- Installed on: The DBMS(s) on which the rule is currently installed.
- Rule Actions: The actions to take if the rule criteria are met.
- Level: The level of the rule: forbidden violation, medium level violation, low level violation, notice level rule or information level rule.

7.3.2 vPatch Rules

vPatch rules are listed in the vPatch tab. Due to the critical function of detecting known vulnerabilities and attacks on the DBMS, vPatch rules cannot be deleted, however they can be disabled, installed on or removed from DBMSs and DBMS Groups. Each vPatch rule has the following properties:

- System ID: The ID number of the rule.
- Name: The name of the rule.

- Description: A short description of the rule.
- Exception: Any exception added by the user (normally to prevent false positives).
- Action: The specific action to be taken when the conditions of the vPatch rule are met.
- DBMSs & Groups:
    - DBMSs: The DBMS(s) on which the rule is installed.
    - Action: The specific action to be taken per DBMS when the conditions of a specific vPatch rule are met.
- Tags: The tag(s) assigned to this rule.
- Enable Rule: If selected, the rule is enabled.

7.3.3 Custom Rules

Based on the organization's ongoing monitoring of potential risks, custom rules can be defined to provide protection against activity that is considered suspicious according to the IT policy and to help protect specific DBMSs according to their functionality. For example, an Administrator may want to monitor access to sensitive tables in an Human Resources (HR) DBMS, such as tables that contain employee compensation information, or they may want to protect against the usage of SQL query tools that are not allowed in the organization on production databases.

Administrators can create and enable custom rules that determine how statements received by the DBMS are handled. Rules can be used to allow statements that match (“white list”), or they can be used to generate alerts regarding statement that do not match the policy (“black list”). A rule can also be used to automatically terminate potentially dangerous sessions.

Each rule consists of one or more comparator statements. The relationship between multiple comparator statements is based on Boolean logic, using AND, OR, or NOT.

Administrators can define exceptions to a rule that does not allow certain conditions by creating an Allow rule for the exception case and placing it before the rule in the Rules list. Administrators can also create an exception within the rule itself.

The order of the rules in the Custom Rules list is important. The first rule that is matched is the rule that is applied to the statement. If a statement does not match any of the existing rules, the statement is allowed. Incoming statements are checked against the vPatch Rules list before they are checked against the Custom Rules list.

7.3.4 Rule Actions

Actions can be defined for any type of rule (i.e. vPatch or custom). When the conditions of the rule are met the Administrator can define the specific action to be taken per monitored DBMS. Alerts are enabled per rule; and you can define only how the alert is handled for the selected DBMS. The following types of actions may be configured:

- **Send Alert to the console** having a priority of either Low, Medium or High
- The rule may be preconfigured to **terminate the user session,** and optionally, the user can also be **quarantined** for a predefined number of minutes during which users will be prevented from reconnecting.

7.4 Vulnerability Assessment

The TOE provides the capability of performing VA scans against monitored DBMSs to identify a wide range of risks and problems. The vulnerability assessment TSF is comprised of 3 components: VA tests, VA scans and VA results.

7.4.1 VA Tests

A VA scan includes one or more tests. A test comprises specific checks that are to be performed against the database. In addition to using the predefined (out-of-the-box) VA tests, an Administrator can create customized VA tests to suit the needs of their organization. These custom tests can be added to preconfigured test groups.

Custom tests can be assigned to the Custom or Data Discovery categories. Custom VA tests can be used to identify the existence of a specific condition or vulnerability, based on a Yes/No test, or they can return a set of relevant data. Data Discovery is used when the rule is designed to discover particular tables/columns in the database. Choosing this category is essential if the Administrator wants to later turn the results into rule objects, to assist in the definition of new rules.

7.4.2 VA Scans

VA scans are based on predefined and/or custom VA tests and are driven by compliance requirements and organizational policy. The TOE enables the configuration of VA scans of the DBMS(s) to identify a wide range of risks and problems, such as weak passwords or missing patches.

The Administrator can configure multiple VA scans to be performed against one or more DBMSs. A VA scan runs one or more groups of tests on the DBMS. VA scans can be scheduled in advance at set time intervals or they can be run on demand. The available test groups are pre-configured, with the exception of the Custom test group that contains any customized tests defined in the VA Tests page. The Administrator can disable specific tests within a test group for a specific scan.

7.4.3 VA Results

After running a VA scan, McAfee Database Security Vulnerability Manager provides detailed information about the scan findings via the Web Console. The administrator can then resolve identified findings in accordance with organizational policy and procedures. Scan results contain the following information:

- Level: The level of the scan result, which can be low, medium, high, notice or information result
- DBMS: The name of the DBMS for which the result was returned.
- Time: The date and time of the scan result.
- Resolution: The state of the scan result (Unresolved, Resolved, False positive, and so on).
- Test: The name(s) of the test (s) that returned the results.
- Action(s): Resolve the result by changing its resolution state

7.5 Identification & Authentication

On the management system, the TOE requires users to identify and authenticate themselves before accessing the TOE software. User accounts must be defined within McAfee Database Security Server through the Web Console. No action can be initiated before proper identification and authentication (I&A). Each TOE user has security attributes associated with their user account that define the functionality the user is allowed to perform.

Users must log in to the TOE with a valid user name and password supplied via a GUI before any access is granted to TOE functions or data. When the credentials are presented by the user, the TOE determines if the user is defined and their status is active. If not, the login process is terminated and the login GUI is redisplayed.

If the user's password is successfully authenticated, the TOE grants access to the Web Console and therefore the TOE functionality. If the authentication is not successful, the login GUI is redisplayed. Upon successful login, the Administrator status and the union of all the permissions from the permission sets from the user account configuration are bound to the session. Those attributes remain fixed for the duration of the session (until the user logs off). If the attributes for a logged in user are changed, those changes will not be bound to a session until the next login by the user.

7.6 Management

The TOE's Management Security Function provides administrator support functionality that enables a user to configure and manage TOE components. Management of the TOE may be performed via the Web Console. Management permissions are defined per-user.

The TOE provides functionality to manage the following:

1. User Account management
2. Permission Set management
3. Alert Archive management
4. History List management
5. Rule management
6. Alert management
7. Sensor management
8. Security Dashboard management
9. VA management

Each of these items is described in more detail in the following sections.

7.6.1 User Account Management

Each user authorized for login to the TOE must be defined via the web console on the McAfee Database Security Server. Only authorized Administrators may perform user account management functions (create, view, modify and delete). For each defined account, the following information is configured:

1. User name
2. First Name
3. Last Name
4. Status: active or inactive
5. Password
6. User role
7. Permission sets granted to the user, including the list of DBMS groups and DBMSs for which the user is authorized to view alerts

One or more permission sets may be associated with an account. Read Only users can view all screens and settings, but cannot make changes to the TSF data or settings. McAfee Database Security Operators can perform operations in the system, but cannot change the security policy and related objects. Policy Creators can create and edit rules, and configure other system components, but cannot view alerts. Read Only Alert users have read-only access to the Security Dashboard and the Alerts list.

7.6.2 Permission Set Management

A permission set is a group of permissions that can be granted to any users by assigning it to those users' accounts. One or more permission sets can be assigned to users.

Permission sets only grant rights and access — no permission ever removes rights or access. When multiple permission sets are applied to a user account, they aggregate. For example, if one permission set does not provide any permissions to server tasks, but another permission set applied to the same account grants all permissions to server tasks, that account has all permissions to server tasks.

When a new sensor is installed on a DBMS, it may add one or more groups of permissions to the permission sets. Initially, the newly added section is listed in each permission set as being available but with no permissions yet granted. The McAfee Database Security Operators can then grant permissions to users through existing or new permission sets.

McAfee Database Security Operators may create, view, modify and delete permission sets. Each permission set has a unique name so that it can be appropriately associated with users. When a permission set is created or modified, the permissions granted via the permission set may be specified by McAfee Database Security Operators.

7.6.3 Alert Archive Management

McAfee Database Security Operators may configure the length of time alerts are to be archived either automatically at predefined time periods (by hours, days, weeks or months) or manually. The age of the alerts to be archived is also specified by the McAfee Database Security Operator.

The alerts may also be purged manually by a McAfee Database Security Operator using the web console to specify that all events older than a specified date are to be deleted. This is a one-time operation and the date specified is independent of the time period specified for automatic purging.

7.6.4 History List Management

The history list captures all user actions and stores them on the Server's external database (provided by the IT Environment). A McAfee Database Security Operator may configure the length of time history entries are to be saved. Entries beyond that time are automatically purged.

7.6.5 Rule management

Authorized users can perform the following management functions on the rule set:

- View the rules per DBMS or as a complete grouping for all monitored DBMSs
- Filter the rules list to display only those rules that match specific criteria, for example, DBMS name or group, tags or compliance type.
- Enable or disable rules depending if they are ready t be deployed or are still under development
- Manage vPatch rules by disabling, installing on or removing from DBMSs and DBMS groups. Management functions on vPatch rules include:

  - Configure the Action for vPatch rules to define the alert level and the action to be taken when the conditions of a specific vPatch rule are met (send alert to console, terminate session and so on). Additional properties of a vPatch rule cannot be modified.
  - Configure the Action for a DBMS to set the specific action to be taken per DBMS when the conditions of a specific vPatch rule are met. Alerts are enabled per rule; you can define only how the alert is handled for the selected DBMS.

- Manage Custom Rules including:
  - Creating custom rules
  - Cloning rules for easier creation of subsequent rules
  - Changing the order of the rules to ensure the organizations monitoring policy is correctly enforced
- Define rule objects so they can be used as components in other rules.
- Create an alert rule based on application mapping results.
- Define exceptions to custom rules
- Define tags and attach them to rules so they can be used to apply multiple rules to a DBMS
- View rule revisions made at any specific point in time. Parameters stored for each revision include the type of revision, date of revision, creator of the revision, name of the rules that were modified.

7.6.6 Alert management

Authorized users can perform the following management functions on the alerts list:

- View the alerts list and the details for individual alerts
- Filter the alerts list to display only those alerts that match specific criteria, for example, DBMS name or group.
- Handle alerts to take appropriate action as described in section 7.1.1
- Generate alert reports
- Archive alerts as described in section 7.6.3

7.6.7 Sensor management

McAfee Database Security Sensors are responsible for monitoring access to the DBMS(s) and sending transaction data to the McAfee Database Security Server. After installation, a sensor needs to be approved before it can begin active monitoring of a DBMS.

McAfee Database Security Operators perform the following management functions with the sensors:

- View the sensors list and the details for individual sensors
- Approve a sensor so it can begin active monitoring of the DBMS
- Approve the DBMS(s) to allow rules to be applied in accordance with the organization monitoring policy
- Starting and stopping the monitoring of the DBMS(s)

7.6.8 Security Dashboard management

The McAfee Database Security Dashboard displays a wide range of statistical data regarding the status of alerts, DBMS monitoring, security updates, and rules.

Authorized users can set the time interval of the data to be displayed in the Dashboard by selecting the relevant time period at the top of the page, for example, Last 10 min, Last hour, Last week, and so on.

7.6.9 VA management

Authorized users can perform the following management functions on the results of VA scans:

- Viewing the VA results
- Filter the VA results list to display only those results that match specific criteria, for example, DBMS name or group.
- Handle VA results to resolve one or more results
- Archive VA results in a compressed and stored archive file. Archived results do not appear in the VA Results list unless the archive file is reloaded.

7.7 Audit

The TOE's Audit Security Function provides auditing of management actions performed by users (administrators). Authorized users may review the audit records via the Web Console. The TOE utilizes four different types of audit logs to record events as they occur:

1. **Alert Archive** which stores all the alerts generated by the sensors (discussed in section 7.6.3).

2. **History List** which captures all user actions and stores them on the Server's external database (provided by the IT environment).

3. **System Messages** log which lists the system messages generated by the system in response to various conditions and events in the system, for example, when a sensor stops communicating with the server or when a license is about to expire.

4. **Rule Revisions** enables users to view the state of rules at any specific point in time and the revisions made to rules over time.

The auditable events are specified in the Audit Events and Details table in the FAU_GEN_EXT.1 section.

Audit Log entries display in a sortable table. For added flexibility, you can also filter the log so that it only displays failed actions, or only entries that are within a certain age. The History List displays the following information:

- Action: The type of action taken (for example, Modify User Rule, Resolve Alert, Approve Sensor, or Change Role).
- Modified by: The name of user who performed the action.
- Modify date: The date and time of the action.
- Parameters: An icon, which when clicked, enables you to view the details of the action.

The System Messages List displays the following information:

- Severity: The level of severity (Low, Medium, or High).
- Subject: The subject of the message.
- Body: The text content of the message.
- Creation Date: The date and time when the message was created.

The Audit Log entries are automatically purged based upon a user-configured age. Other than automatic purging, no mechanisms are provided for users to modify or delete entries. The audit log entries are stored in the external database.

Alert data is automatically purged according to the configured Data Retention parameters. If the storage capacity of the database is exceeded, old alert records are overwritten with new alert records. The TOE does not provide any mechanism to modify audit data, and the only mechanism to delete audit data is the automatic purging based on the configured Data Retention parameters.

7.8 Protected System Data Transfer

The TOE consists of distributed components. Server to sensor communication relies upon cryptographic functionality (Transport Layer Security) provided by the TOE to protect the information exchanged from unauthorized disclosure or unauthorized modification. Encrypted sessions are implemented using a secure connection using TDES or AES encryption algorithms supported by the TOE. The TOE provides cryptography via CAVP-validated algorithm implementations, and the cryptographic module fulfills the requirements of FIPS 140-2 Overall Level 2 (see certificates TBD and TBD).