Security Target

McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1

Document Version 2.2

February 16, 2016

Security Target: McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1

Prepared For:

McAfee, Inc.

2821 Mission College Blvd.

Santa Clara, CA 95054

www.mcafee.com

Prepared By:

38North Security, LLC

2020 Pennsylvania Ave NW, Suite 254

Washington, DC 20006

www.38northsecurity.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1. 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 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1
ST Revision	2.2
ST Publication Date	February 16, 2016
Author	38North Security

1.2 TOE Reference

TOE Reference	McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1, with these extensions installed: • McAfee Database Activity Monitoring extension Version 5.1.3 • McAfee Vulnerability Manager for Databases extension Version 5.1.3 • McAfee Rogue Database Detection extension Version 1.0.9 • McAfee Advanced Management Core extension Version 1.0.9 McAfee Database Security Sensor Version 5.1.2 McAfee Agent Version 4.8.0 McAfee Virtual Patching for Databases Version 5.1.3
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

SECTION	TITLE	DESCRIPTION
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
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 <u>underlined</u> 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

TERM	DEFINITION
AD	Active Directory
CC	Common Criteria version 3.1 (ISO/IEC 15408)
CPU	Central Processing Unit
DAM	McAfee Database Activity Monitoring
DBMS	DataBase Management System
DNS	Domain Name System
DSS	Data Security Standard
DVM	McAfee Vulnerability Manager for Databases
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
GUI	Graphical User Interface
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
VA	Vulnerability Assessment
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 via McAfee ePolicy Orchestrator (ePO) to generate events 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, send an event, 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 as defined in Table 3) and help prevent attacks against known vulnerabilities. In addition, you can define custom rules to define the level of monitoring and generated events, 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 managed 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 Agent:** A software agent residing on the DBMS host server which provides secure communication between the sensor on the managed DBMS and the ePO server. The McAfee Agent performs the following services while collaborating with the sensor:
    - Gathers information and events from managed DBMSs and sends them to the ePO server.

  - Installs sensors on managed DBMSs.
  - Provides the monitoring policies to the sensor component installed on managed DBMSs.
  - Updates security content such as the vPatch rules enforced by the sensor component.

- **McAfee ePolicy Orchestrator (ePO)**: An application executing on a dedicated server which manages and securely communicates with all installed sensors via the McAfee Agent. A centralized but distributed architecture allows the agent software to be centrally managed and yet decrease network traffic required to manage systems. The ePO server software utilizes an external database to store all data created and used by ePO. The ePO server provides:

  - The management interface and functionality for the administrators of the TOE.
  - Centralized audit collection and review functionality, including the ability to run queries and reports on event data received from the managed systems.
  - Database security-specific functions for monitoring policy management and vulnerability assessment.

  In order to comply with the evaluated configuration, the ePO server requires the installation of several extensions to enable both the Database Activity Monitoring (DAM) and Vulnerability Manager for Databases (DVM) functionality (refer to Table 3 – Evaluated Configuration for the TOE for applicable versions):

  - McAfee DAM extension: adds DAM-specific functionality to ePO including various submenus and actions which define system parameters, configuration settings, policy settings and reporting options. Three new Database Security predefined user roles are also added.
  - McAfee DVM extension: adds the DVM-specific functionality to ePO including various submenus and actions which define server tasks, system parameters, configuration settings, policy settings, and reporting options. The three Database Security predefined user roles (added by the DAM extension) are added if the DAM extension has not yet been installed.
  - McAfee Rogue Database Detection extension: used by DAM for managing discovered DBMSs if they are inadvertently deleted from the System Tree. This extension is not used by DVM.
  - McAfee Advanced Management Core extension: used to support the credential sets in both DAM and DVM.

  It is also noted that McAfee Virtual Patching for Databases must be separately licensed in order to comply with the evaluated configuration (refer to Table 3 – Evaluated Configuration for the TOE for the applicable version). McAfee Virtual Patching for Databases is a content deliverable

managed through the McAfee DAM extension. As discussed above, it provides predefined vPatch rules used to prevent attacks exploiting known vulnerabilities.

The McAfee Database Security Sensor monitors access to the DBMS and sends all the transaction data to ePO via the McAfee Agent (no data is stored on the sensors or the agent). Monitoring functionality is provided by the Database Activity Monitoring extension to ePO. Based on the monitoring policies defined for each managed DBMS, the ePO server logs the transaction, generates an event, 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), DAM events, DVM events, and other system data.

Vulnerability assessment functionality is provided by the McAfee Vulnerability Manager for Databases extension to ePO 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. All results are transferred back to the ePO external database where they can be queried and added to reports. VA scans are conducted by ePO over a JDBC connection with the target DBMS and do not utilize the McAfee Agent.

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 on the ePO management console. 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/Agent and ePO 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 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 Agent:** A software agent residing on the DBMS host server which provides secure communication between the sensor on the managed DBMS and the ePO server.

3. **McAfee ePolicy Orchestrator (ePO)**: An application executing on a dedicated server which manages and securely communicates with all installed sensors via the McAfee Agent. The ePO server is configured with several extensions (see below) which enable the database monitoring and vulnerability assessment functionality. The ePO server software utilizes an external database provided by the IT environment to store all data created and used by ePO.

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 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1, with these extensions installed: • McAfee Database Activity Monitoring extension Version 5.1.3 • McAfee Vulnerability Manager for Databases extension Version 5.1.3 • McAfee Rogue Database Detection extension Version 1.0.9 • McAfee Advanced Management Core extension Version 1.0.9 McAfee Database Security Sensor Version 5.1.2 McAfee Agent Version 4.8.0 McAfee Virtual Patching for Databases Version 5.1.3
IT Environment	Specified in the following: • Table 4 – Management System Component Requirements • Table 5 – Supported DBMS and McAfee Agent Platforms • Table 6 – 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 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1 (this document) • Product Guide: McAfee Database Activity Monitoring 5.1.0 • Product Guide: McAfee Vulnerability Manager for Databases 5.1.0 • Product Guide: McAfee ePolicy Orchestrator 5.3.0 Software • Product Guide: McAfee Agent 4.8.0 • Installation Guide: McAfee ePolicy Orchestrator 5.3.0 Software • User Guide: McAfee ePolicy Orchestrator 5.3.0 Software FIPS Mode • Operational User Guidance and Preparative Procedures Supplement: McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1

Table 3 – Evaluated Configuration for the TOE

The evaluated configuration consists of a single instance of the management system (with ePO) and one or more instances of the managed systems (with McAfee Agent and the Sensor software). McAfee Database Activity Monitoring, McAfee Vulnerability Manager for Databases and Virtual Patching for Databases must all be licensed to comply with the evaluated configuration.

ePO supports ePO authentication, Windows authentication and Certificate-based authentication of user account credentials. The evaluated configuration requires the use of ePO authentication only.

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.

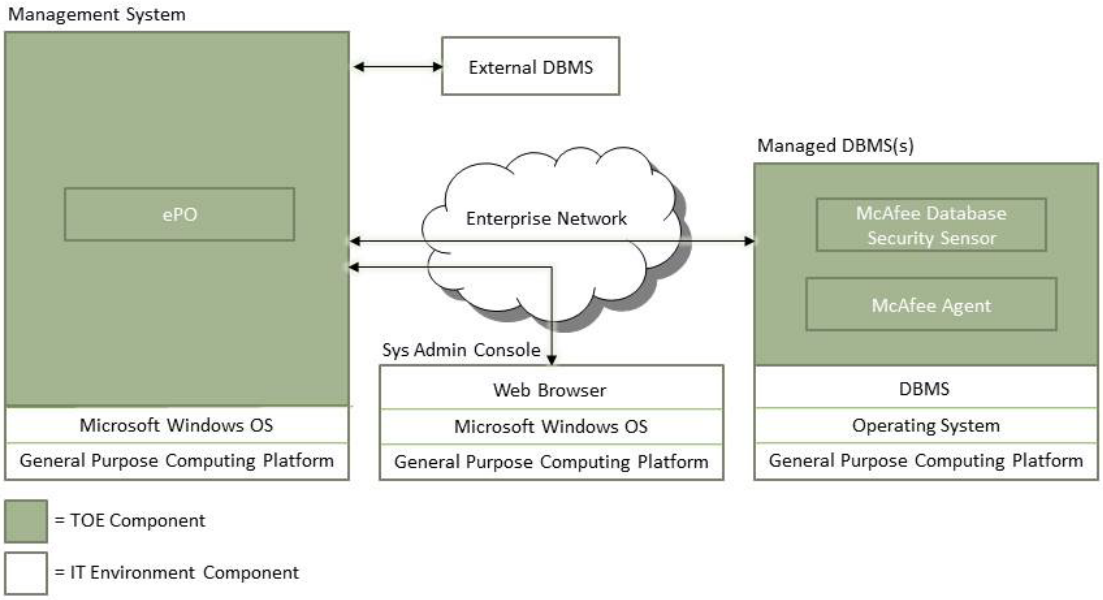

Figure 1 – TOE Boundary

The following specific configuration options apply to the evaluated configuration:

1. The monitoring of Teradata DBMSs has been excluded from the evaluated configuration.
2. DBMSs executing on the following operating systems have been excluded from the evaluated configuration: Z/OS, AS/400, IBM AIX, HP-UX.
3. The IT Environment provides an external DBMS for DAM/DVM event storage, and other system data.
4. Certificate, Windows and LDAP user authentication methods have been excluded from the evaluated configuration.

5. The utilization of syslog servers, Windows event logs, XML API, email or Twitter accounts to send events and/or system messages has been excluded from the evaluated configuration.
6. Updates to the TOE software are not permitted in the evaluated configuration.
7. Operating System (OS)-level vulnerability tests have been excluded from the evaluated configuration.[1]
8. Running the McAfee ePO server in cluster mode is not permitted in the evaluated configuration.
9. The use of predefined compliance rule sets have been excluded from the evaluation.[2]
10. The protection of TSF data transmitted between (1) the administrator's web browser and the ePO server; and (2) the ePO server and the DBMSs subject to vulnerability scanning (DVM Scans), has been excluded from the evaluation.

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.

The platform on which the ePO 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
Processor	64-bit Intel Pentium D or higher; 2.66GHz or higher
Memory	4 GB available RAM recommended minimum
Free Disk Space	5 GB — Recommended minimum
Operating System (64-bit)	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
DBMS	Microsoft SQL Server 2008 R2 Enterprise with Service Pack 1 Microsoft SQL Server 2008 R2 Express with Service Pack 1 Microsoft SQL Server 2008 R2 Standard with Service Pack 1 Microsoft SQL Server 2008 R2 Workgroup with Service Pack 1
Required Software	Microsoft .NET Framework 2.0 or later Microsoft Visual C++ 2005 SP1 Redistributable Microsoft Visual C++ 2008 Redistributable Package (x86) Microsoft XML Core Services (MSXML) 6.0

Table 4 – Management System Component Requirements

[1] 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.

[2] 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.

McAfee Database Security Sensor and McAfee Agent execute 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 2003	Oracle 10.2, 11 Sybase ASE 15, 15.5, 15.7 DB2 9, 10
	Windows Server 2008	Microsoft SQL Server 2005, 2008, 2012 Oracle 10.2, 11.1, 12
	Windows Server 2008 R2	Microsoft SQL Server 2008
	Windows Server 2012	Microsoft SQL Server 2012
Linux (Intel x86, 64-bit)	CentOS 5	Oracle 12
	CentOS 5.5	MySQL 5.1, 5.5, 5.6
Solaris (SPARC, 64-bit)	Solaris 10	Oracle 8, 9, 10, 11, 12 Sybase ASE 15, 15.5, 15.7 DB2 9.5, 9.7, 10.1, 10.5

Table 5 – Supported DBMS and McAfee Agent Platforms

In addition, McAfee Vulnerability Manager for Databases will only execute VA scans on the following supported DBMSs (on the platforms specified in Table 5):

SUPPORTED DBMS PLATFORMS FOR VULNERABILITY ASSESSMENT
Microsoft SQL Server 2000, 2005, 2008, 2012 on all supported OS platforms
Oracle 9g, 10g, 11g on all supported OS platforms
Sybase ASE 15.0 on all supported OS platforms
DB2 LUW 9.1, 9.5, 9.7 on all supported OS platforms
MySQL 5.5 on all supported OS platforms

Table 6 – Supported DBMS Platforms for Vulnerability Assessment Functionality

The management system (ePO) is accessed from one of the following supported Internet web browsers: Mozilla Firefox 10.0 and later, Microsoft Internet Explorer 8.0 and later, Google Chrome 17.0 and later, and Apple Safari 6.0 and later.

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 generate DAM events and/or terminate suspicious activities. DAM events are sent from the McAfee Database Security Sensor to the McAfee Agent which then securely forwards the events to the ePO server for analysis where they are stored in the external database (provided by the IT environment) for subsequent analysis. Events and reports are accessed via ePO.
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 event generated 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, send an event, 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 events to be generated, 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 checks 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 ePO management interface. 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 ePO. 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 is performed via the ePO management interface. 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 ePO management interface.
Protected Data Transfer	The TOE consists of distributed components. ePO server to sensor communication relies upon cryptographic functionality provided by the TOE to protect the information exchanged from disclosure or modification.

Table 7 – 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
Application Map	A map of all applications running on monitored DBMSs, including the users running the applications.			✓

TSF Data	Description	AD	UA	GE
Database Security Dashboard	A wide range of statistical data regarding the status of DAM events, DAM sensors, DBMS monitoring, DVM events, including Top 10 events, Top 10 scans, and collated events by category, DBMS, severity and type.			✓
DAM Event	An event generated when the preconditions of an active rule have been met on a monitored DBMS.			✓
DAM Events Log	Lists all generated DAM events including the event ID and severity, as well as information on the policy that detected the event on the monitored DBMS.			✓
Data Retention	Parameters controlling the length of time events are saved in the database.			✓
DVM Check	A predefined and/or custom test used during a DVM Scan that is to be performed against managed DBMSs.			✓
DVM Event	An event (result) generated during a DVM Scan including a description of the vulnerability, its implications, and an SQL Fix (if available).			✓
DVM Events Log	Lists all DVM Scan results (DVM Events) including the event ID and severity, as well as information on the scan and specific check that detected the event.			✓
DVM Scan	D VM scans are based on one or more predefined and/or custom DVM checks and are driven by compliance requirements and/or organizational policy.			✓
ePO User Accounts	ePO user name, role, authentication type, logon status, and permission set for each user authorized to access TOE functionality on the management system.	✓		
Exceptions	Exceptions may be applied to the rule set or individual rules so that specific conditions do not trigger the rule.			✓
Groups	Node on the hierarchical System Tree that may contain subordinate groups or systems.			✓
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.			✓
Quarantine List	List of all DBMSs that have been quarantined in accordance with organizational policy.			✓
Queries	Configurable objects that retrieve and display data from the ePO external database.			✓
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.			✓
Server Settings	Control how the ePO server behaves.			✓

TSF Data	Description	AD	UA	GE
System Information	Information specific to a single managed system (e.g. Internet address) in the System Tree.			✓
System Tree	A hierarchical listing of all systems managed by ePO, including all monitored and scanned DBMSs.			✓
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.			✓
Threat Event Log	Lists all threat events generated by the managed systems. The DAM and DVM Event Logs are a subset of the Threat Event Log.			✓

Table 8 – 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 ePO server executes is dedicated to that purpose. The McAfee Database Security Sensor and McAfee Agent execute on the DBMSs; these components only perform 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. Communication between the components 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 9 – 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 10 – 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 11 – 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	The authorized administrator's web browser will use HTTPS to protect management sessions.
A.SSLDBMS	DBMS administrators will ensure that each managed DBMS has been configured to support Secure Sockets Layer (SSL) connections over its network interface.

Table 12 – 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 13 – 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, the external database 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 14 – 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 15 – 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	The authorized administrator's web browser will use HTTPS to protect management sessions. 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 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. The OE.SD_PROTECTION objective provides for the capability to protect system data via mechanisms outside the TSC.

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 OE.SD_PROTECTION objective provides for the capability to protect system data via mechanisms outside the TSC. 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 16 – 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 17 – 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*].	

5.2 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(1-4)	Cryptographic Key Generation
	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

Table 18 – 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 (events) are purged when the audit trail exceeds the predefined age for the ePO Threat Event Log.	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

Table 19 – 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, Database Security Administrator, Database Security Operator, Database Security Reviewer, and Global Reviewer* 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 **via interfaces within the TSC**.

FAU_STG.1.2 The TSF shall be able to prevent unauthorized modifications to the audit records in the audit trail **via interfaces within the TSC**.

Application Note: The TOE is only able to restrict access to the external database from within the TSC. Access to the database from outside the TSC is addressed by OE.SD_PROTECTION.

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

FAU_STG.3.1 The TSF shall purge the oldest events from the external database if the audit trail exceeds the specified age configured for the ePO Threat Event Log.

Application Note: This requirement only applies to the purging of the DAM/DVM events.

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_CKM.1(1) Cryptographic Key Generation (ePO AES)

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*CTR_DRBG for deterministic random bit generation*] and specified cryptographic key sizes [*256 bits for encryption/decryption*] that meet the following: [*NIST Special Publication 800-90 (CAVP algorithm certificate #540)*].

6.1.2.2 FCS_CKM.1(2) Cryptographic Key Generation (ePO RSA)

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*CTR_DRBG for deterministic random bit generation*] and specified cryptographic key sizes [*2048 bits for key transport*] that meet the following: [*NIST Special Publication 800-90 (CAVP algorithm certificate #540)*].

6.1.2.3 FCS_CKM.1(3) Cryptographic Key Generation (MA AES)

FCS_CKM.1.1(3) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*PRNG for random number generation*] and specified cryptographic key sizes [*256 bits for encryption/decryption*] that meet the following: [*FIPS 186-2 (CAVP algorithm certificate #270)*].

6.1.2.4 FCS_CKM.1(4) Cryptographic Key Generation (MA RSA)

FCS_CKM.1.1(4) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*PRNG for random number generation*] and specified cryptographic key sizes [*2048 bits for key transport*] that meet the following: [*FIPS 186-2 (CAVP algorithm certificate #270)*].

6.1.2.5 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: [*FIPS 140-2 level 1 requirements for key zeroization*].

6.1.2.6 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 as described below*] and cryptographic key sizes [*multiple key sizes described below*] that meet the following: [*multiple standards described below*].

Table 20 – Cryptographic Operations

OPERATION	ALGORITHM	KEY SIZE IN BITS	STANDARDS
Key Transport	RSA encrypt/decrypt	2048	Allowed in FIPS mode
Symmetric encryption and decryption	Advanced Encryption Standard (AES) (operating in ECB or CBC mode)	256	FIPS 197

OPERATION	ALGORITHM	KEY SIZE IN BITS	STANDARDS
Secure Hashing	SHA-384	Not Applicable	FIPS 180-3

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) Logon Status (enabled or disabled);

c) Authentication Configuration (must be configured for ePO);

d) Password;

e) Assigned Permissions; and

f) *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 Database Security Administrator*.

Application Note: System data collection and reaction in this context refers to the collection and reaction functions performed by Database Activity Monitoring. Vulnerability assessment management functions are performed by the ePO 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 and Database Security Administrator*.

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 *Database Security Administrator, Database Security Operator, Database Security Reviewer, and Global Reviewer 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 **DSA** = Database Security Administrator, **DSO** = Database Security Operator, **DSR** = Database Security Reviewer, and **GR** = Global Reviewer. Note the Admin role is not shown throughout the table below to enhance clarity of the other user roles.*

Table 21 – TSF Data Access Permissions for Authorized Users

TSF Data	Change Default	Query	Modify	Delete
Application Map	DSA, DSO, DSR	DSA, DSO, DSR	DSA, DSO, DSR	DSA, DSO, DSR
Database Security Dashboard	Public: DSA Private: DSA, DSO, DSR	Public: DSA, DSO, DSR, GR Private: DSA, DSO, DSR	Public: DSA Private: DSA, DSO, DSR	Public: DSA Private: DSA, DSO, DSR
DAM Event		DSA, DSO, DSR		DSA, DSO (via Threat Event Log)
DAM Events Log	DSA, DSO	DSA, DSO, DSR	DSA, DSO	DSA, DSO (via Threat Event Log)
Data Retention	DSA, DSO	DSA, DSO	DSA, DSO	DSA, DSO
DVM Check	DSA, DSO	DSA, DSO, DSR	DSA, DSO	DSA, DSO (custom checks only)
DVM Event		DSA, DSO, DSR		DSA, DSO (via Threat Event Log)

TSF Data	Change Default	Query	Modify	Delete
DVM Events Log	DSA, DSO	DSA, DSO, DSR	DSA, DSO	DSA, DSO (via Threat Event Log)
DVM Scan	DSA, DSO	DSA, DSO, DSR Limited: GR	DSA, DSO (user-created scans only)	DSA, DSO (user-created scans only)
ePO User Accounts	Admin only	Admin only	Admin only	Admin only
Exceptions	DSA	DSA, DSO, DSR, GR	DSA	DSA
Groups	DSA, DSO	DSA, DSO, DSR, GR	DSA, DSO	DSA, DSO
Permission	Admin only	Admin only	Admin only	Admin only
Permission Set	Admin only	Admin only	Admin only	Admin only
Policy	DSA	DSA, DSO, DSR, GR	DSA	DSA
Quarantine List		DSA, DSO, DSR	DSA, DSO	DSA, DSO
Queries	Private Queries: DSA, DSO, DSR	Public Groups: DSA, DSO, DSR, GR Private Queries: DSA, DSO, DSR	Private Queries: DSA, DSO, DSR	Private Queries: DSA, DSO, DSR
Rule	DSA	DSA, DSO, DSR, GR	DSA	DSA
Rule set	DSA	DSA, DSO, DSR, GR	DSA	DSA
Server Settings	All: Admin	All: Admin Limited: DSA, DSR, GR	All: Admin Limited: DSA, DSR	All: Admin
System Information	DSA, DSO	DSA, DSO, DSR, GR	DSA, DSO	DSA, DSO
System Tree	DSA, DSO	DSA, DSO, DSR, GR	DSA, DSO	DSA, DSO
Tags	DSA, DSO	DSA, DSO, DSR, GR	DSA, DSO	DSA, DSO
Threat Event Log	DSA, DSO	DSA, DSO, DSR, GR	DSA, DSO	DSA, DSO

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) Event archive management,

d) Audit log management,

e) Rule management,

f) Event management,

g) Sensor management,

h) 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, Database Security Administrator, Database Security Operator, Database Security Reviewer, and Global Reviewer*.

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 production separation of duties is enforced through only using the following roles: Database Security Administrator, Database Security Operator, Database Security Reviewer, and Global Reviewer.

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: FPT_ITT.1 only applies to the transmission of TSF data between the McAfee Agent (installed on the managed DBMS) and the ePO server. The protection of TSF data transmitted between (1) the administrator's web browser and the ePO server; and (2) the ePO server and the DBMSs subject to vulnerability scanning (DVM Scans), has been excluded from the evaluation.

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, destination address

COMPONENT	EVENT	DETAILS
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 22 – 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) Signature*;* and

b) No other functions.

Application Note: Signature analysis is provided primarily through vPatch rules which can prevent attacks against known vulnerabilities. Custom rules can also be created to provide 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 event), 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 event 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, Database Security Administrator, Database Security Operator, Database Security Reviewer, and Global Reviewer* with the capability to read *events* 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 **via interfaces within the TSC**.

IDS_ STG.1.2 The System shall protect the stored System data from modification **via interfaces within the TSC**.

Application Note: The TOE is only able to restrict access to the external database from within the TSC. Access to the database from outside the TSC is addressed by OE.SD_PROTECTION.

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.

6.2 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

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
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 23 – 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(1-4)	No other components	FCS_CKM.2 or FCS_COP.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

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
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

Table 24 – 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		✓									✓		

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
FCS_CKM.1(1-4)									✓	✓			
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	✓					✓				✓			✓

Table 25 – Mapping of TOE SFRs to Security Objectives

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

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].

OBJECTIVE	RATIONALE
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 age, the oldest events are purged 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].
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 TOE may change default, query, modify, and/or delete TSF data as per their assigned permissions [FMT_MTD.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1].

OBJECTIVE	RATIONALE
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(1-4), 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 TOE may change modify and/or delete TSF data as per their assigned permissions [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(1-4), FCS_CKM.4, FCS_COP.1] between TOE components.
O.OFLOWS	The TOE must appropriately handle potential TOE data storage overflows. The TOE must take action in case of possible loss of events in the audit trail exceeds a predefined age [FAU_STG.3].
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 TOE may change default, query, modify, and/or delete TSF data as per their assigned permissions [FMT_MTD.1].

Table 26 – 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 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1
ADV_TDS.1: Basic Design	Basic Design: McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1
ALC_DEL.1: Delivery Procedures	Secure Delivery Processes and Procedures: McAfee Software Delivery Process Document Version 1.0
ALC_FLR.2: Flaw Reporting Procedures	Product Flaw Remediation Process Document Version 1.3
ATE_COV.1: Evidence of Coverage	Security Testing: McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1
ATE_FUN.1: Functional Testing	Security Testing: McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ATE_IND.2: Independent Testing – Sample	Security Testing: McAfee Database Security 5.1 (Database Activity Monitoring 5.1.2 and Vulnerability Manager for Databases 5.1.3) with ePolicy Orchestrator 5.3.1

Table 27 – 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							✓	

SFR \ TSF	DBMS Transaction Monitoring	DBMS Session Termination & User Quarantine	Rule-based Policy Enforcement	Vulnerability Assessment	Identification & Authentication	Management	Audit	Protected System Data Transfer
FCS_CKM.1(1-4)								✓
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	✓					✓	✓	

Table 28 – 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 event age has been reached, the TOE will purge the oldest events in the external database.

SFR	SF AND RATIONALE
FCS_CKM.1(1-4)	**Protected System Data Transfer** – The TOE provides secure communications between the ePO server and monitored DBMSs, in part, through the generation of cryptographic keys used to establish encrypted sessions for the safe passage of TSF data.
FCS_CKM.4	**Protected System Data Transfer** – The TOE provides secure communications between the ePO server and monitored DBMSs, 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 ePO server and monitored DBMSs 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 Database Security Administrator roles.
FMT_MOF.1 (2)	**Management** - The ability to modify the behaviour of the functions of vulnerability assessment management are restricted to the Admin and Database Security Administrator roles.
FMT_MTD.1	**Management** – The user role (Admin, Database Security Administrator, Database Security Operator, Database Security Reviewer, and Global Reviewer) 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 the ePO 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 events are stored in the external database.

SFR	SF AND RATIONALE
IDS_ANL.1	**DBMS Transaction Monitoring/Vulnerability Assessment** – The TOE analyses the results of the DAM and DVM events performed to indicate vulnerabilities on each monitored DBMS. DAM and DVM events are stored in the external database.
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 events 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 event information from unauthorized deletion and modification via interfaces within the TSC because no mechanism exists for modification.

Table 29 – 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 generate DAM events and/or terminate suspicious activities. Rules are provided by the Rule-based Policy Enforcement TSF.

DAM events are sent from the McAfee Database Security Sensor to the McAfee Agent which then forwards the DAM events to the ePO Server for analysis where they are then stored in the external database (provided by the IT Environment) for subsequent analysis. DAM events, queries and reports are accessed via the ePO server management web-based interface.

7.1.1 DAM Events

DAM events are the primary method of communicating abnormal or suspicious activity to the administrator. DAM events are displayed to the administrator in the DAM Events Log (or the ePO Threat Event Log) which consists of the information needed by the administrator to perform review and take any further action if necessary. Each DAM event contains the following information and/or available actions:

- Execution Time: date and time the event was generated.
- Event ID: identification number of the event.
- Severity: the level of severity associated with the event.
- DBMS Name: the name of the DBMS for which the event was triggered.
- Source IP: The IP address of the user (if available).
- Source Host: the name of the source host.
- User: the operating system user.
- Application: the application that created the SQL statement that triggered the event.
- Cmd Type: The SQL command type.
- Statement: the requested operation (original SQL statement) that triggered the event.
- Rules: the names(s) of the rule(s) that generated the event.

Administrators may create filters to make it easier to sort through the DAM Events Log.

7.1.2 Database Security Dashboard

The administrator monitoring function of the TOE is performed on the ePO server using the Database Security Dashboard. The Database Security Dashboard displays a wide range of statistical data regarding the status of events and DBMS activity. Information displayed in the Database Security Dashboard is cached and automatically refreshed every 5 minutes by default.

The default Database Security Dashboard displays the following types of statistical data:

- Operational status of deployed database monitoring sensors connected to the ePO server
- Database monitoring events summary for the selected time period (default is last 14 days) per DBMS
- DBMS activity monitoring state – depicts the number of DBMSs currently being/not being monitored by deployed sensors
- DBMS monitoring events summary for the selected time period (default is last 7 days) per severity level
- Most active custom rules as defined by the number of events for the selected time period (default is last 7 days) per DBMS
- Most active vPatch rules as defined by the number of events for the selected time period (default is last 7 days) per DBMS

The Database Security Dashboard may be reconfigured to assist in DAM management by creating new monitors from the ePO Monitor Gallery pane.

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 when the relevant precondition(s) of a matching rule has been met. Specifically, 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.

Administrators of the TOE may specify within the rule whether 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, send an event, 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 administrator 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 events to be generated, 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. 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:

- Name: The name of the rule.
- Rule text: The comparator statements (Identifiers, Operators & Literals) that serve as the criteria for matching the rule against the incoming or outgoing SQL statement.
- Monitoring source: the basis for allowing monitoring source types for the rule (source may be memory or network, or both).
- Exceptions: lists any exceptions to the rule. Exceptions are defined in response to false positive results to prevent the rule from identifying a specific behavior as an attack.
- Rule Actions: The actions to take if the rule criteria are met. An action will result in the creation of a DAM event which will be logged to the ePO server. The event severity level (i.e. Info,

Notice, Low, Medium or High) is assigned as the rule action is being defined by the administrator.

- Tags: the tags assigned to the rule.
- Enabled/Disabled: A checkbox used to enable or disable the rule.

7.3.2 vPatch Rules

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 additional properties:

- System ID: The ID number of the rule.
- Description: A short description of the rule.
- DBMS Versions: whether the rule applies to vulnerable versions only or all DBMS versions.
- Confidence: confidence level of the rule (i.e. high, medium, or both).

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 events 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. Events are enabled per rule; and you can define only how the event is handled for the selected DBMS. The following types of actions may be configured:

- **Log to ePO** having an event priority of either Info, Notice, Low, Medium or High
- The rule may also be preconfigured to **terminate 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

McAfee Vulnerability Manager for Databases (DVM) scans multiple databases to identify and evaluate potential risks to the enterprise's sensitive data. DVM discovers databases on the network and determines if the latest patches have been applied. It also tests for common weaknesses such as weak passwords, default accounts, and other common threats.

DVM is an extension for use with McAfee ePO. After installing the extension, DVM is available from the McAfee ePO console. DVM 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. All results are transferred back to the ePO external database where they can be queried and added to reports. DVM scans are conducted by ePO over a JDBC connection with the target DBMS and do not utilize the McAfee Agent.

The vulnerability assessment TSF is comprised of 4 main components: DVM Checks, DVM Scans, DVM Events (results) and the Database Security Dashboard.

7.4.1 DVM Checks

A DVM scan includes one or more checks (tests) to be performed against the database. In addition to using the predefined (out-of-the-box) DVM checks, an administrator can create customized DVM checks to suit the needs of their organization. These custom checks can be added to preconfigured check groups which are arranged into categories.

Check groups are used to include multiple checks in a scan without the need to add them individually. Each check can be assigned to multiple check groups, with the check remaining in its original category. Each check category has a check group of the same name. The check group automatically includes all checks in the corresponding category. All checks in a group are included in a scan when that category is selected in the scan definition.

Custom checks 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.

7.4.2 DVM Scans

DVM scans are conducted by ePO over a JDBC connection with the target DBMS and do not utilize the McAfee Agent. DVM scans are based on predefined and/or custom DVM checks (which can include check groups and categories) and are driven by compliance requirements and organizational policy. The TOE enables the configuration of DVM 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 DVM scans to be performed against one or more DBMSs. A DVM scan runs one or more groups of checks on the DBMS. DVM scans can be scheduled in advance at set time intervals or they can be run on demand.

7.4.3 DVM Events (Results)

After running a DVM scan, all results are transferred back to the ePO external database as DVM events where they can be queried and added to reports. DVM events are displayed to the administrator in the DVM Events Log (or the ePO Threat Event Log) which consists of the information needed by the administrator to perform review and take any further action if necessary. Each DVM event contains the following information and/or available actions:

- Event ID: identification number of the event.
- Execution Time: date and time of scan that detected the event.
- Host: host where event was detected.
- DBMS Name: DBMS where the event was detected.
- Scan Name: name of the scan that detected the event.
- Check Name: name of the check that detected the event.
- Severity: the level of severity associated with the event (i.e. Info, Notice, Low, Medium or High).
- Information: event information.
- Category: event category.
- Result State: event state.
- Username: database user name.

Administrators may create filters to make it easier to sort through the DVM Events Log.

7.4.4 Database Security Dashboard

The Database Security Dashboard displays a wide range of statistical data regarding the status of events and DBMS activity. Information displayed in the Database Security Dashboard is cached and automatically refreshed every 5 minutes by default.

The default Database Security Dashboard displays the following types of statistical data:

- Top Ten Events: displays events most frequently detected in the last 30 days, across all scanned databases, according to the number of findings.
- Top 10 Scans: displays scans that detected the highest number of events in the last 30 days, across all scanned databases, according to the number of findings.
- Unique Events by Category: displays the distribution of unique events by category.
- Unique Events by DBMS and Severity: displays the distribution of unique events by DBMS and severity.
- Unique Events by DBMS and Category: displays the distribution of unique events by DBMS and category.
- Unique Events by DBMS Type: displays the distribution of events by DBMS type.

The Database Security Dashboard may be reconfigured to assist in DVM management by creating new monitors from the ePO Monitor Gallery pane.

7.5 Identification & Authentication

On the ePO management system, the TOE requires users to identify and authenticate themselves before accessing the TOE software. User accounts must first be created on the ePO server by the Administrator. 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 ePO management interface 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 is performed using the ePO management console. Management permissions are defined per-user.

The TOE provides functionality to manage the following:

1. User Account management
2. Permission Set management
3. Event Archive management
4. Audit log management
5. Rule management
6. Event management
7. Sensor management
8. 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 on the ePO management console. Only authorized administrators may perform user account management functions (create, view, modify and delete). For each defined account, the following information is configured:

1. Username;
2. Logon Status (enabled or disabled);
3. Authentication Configuration (must be configured for ePO);
4. Password;
5. Assigned Permissions; and
6. Assigned Role.

One or more permission sets and/or roles may be associated with an account. Installation of the DAM/DVM product extensions adds the following TOE-specific roles (in addition to the **Admin** role which has access to all TOE functions and data):

Database Security Administrator — By default, the Database Security Administrator can create, edit, or delete Scheduler tasks and queries. This user can view and edit all DVM and DAM properties, including permission and policy configurations, dashboards, and the credential catalog. This user can also view, delete, and purge events.

Database Security Operator — By default, the Database Security Operator can view the System Tree and all DVM and DAM properties, the audit log, credential catalog, and can edit the dashboards. This user can also view the events in the Threat Event Log.

Database Security Reviewer — By default, the Database Security Reviewer can view the System Tree, DVM and DAM results, and weak passwords.

In addition to the DAM/DVM-specific roles, the pre-existing ePO role **Global Reviewer** can view policies (for both DAM and DVM), view rules/objects (DAM only), view the System Tree and associated system information, view DVM Scans, view client tasks for (DAM only), view the ePO Threat Event Log, and view the user audit log.

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.

Administrators 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 only be specified by the Administrator.

7.6.3 Event Archive Management

Administrators may load previously archived event files if needed. The events may also be purged manually by an administrator via the ePO Threat Event Log by specifying that all events older than a specified period of time (in days, weeks, months or years) are to be deleted. A query can also be enabled to automate purging of DAM/DVM events every 7 or 14 days as specified by the administrator.

7.6.4 Audit Log Management

The audit log captures all user actions and stores them on the ePO server's external database (provided by the IT Environment). The administrator may configure the length of time audit 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 to 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 event severity level and the action to be taken when the conditions of a specific vPatch rule are met (send event to the ePO Threat Event Log, 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.
- 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 a 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

7.6.6 Event management

Authorized users can perform the following management functions on the DAM/DVM Event Logs:

- View the event logs and the details for individual events
- Filter the events list to display only those events that match specific criteria, for example, DBMS name or group.
- Generate event queries and reports
- Archive, import and purge events 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 ePO server via the McAfee Agent. The McAfee Agent must be installed on the DBMS before the sensor can be deployed. The sensor and agent may be deployed via ePO or locally depending on the environment and associated deployment constraints.

Administrators perform the following management functions with the sensors:

- Define the sensor configuration policy
- Define the DBMS monitoring configuration policy
- Deploy the sensors
- View the sensors within ePO and the details for individual sensors
- Starting and stopping the monitoring of the deployed sensors on the DBMS(s)

7.6.8 Dashboard management

The Database Security Dashboard displays a wide range of statistical data regarding the status of events, DBMS monitoring, and results from DVM scans. Please refer to sections 7.1.2 and 7.4.4 for more information.

7.6.9 VA management

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

- Viewing the DVM events (results).
- Filter the DVM Events Log to display only those results that match specific criteria, for example, DBMS name or group.
- Act accordingly in response to DVM events.

- Archive DVM events to file. Archived results do not appear in the DVM Event Log unless the archive file is reloaded.

7.7 Audit

The TOE's audit security function provides auditing of management actions performed by authorized users. Authorized users may review the audit records via the Audit Log. The TOE utilizes two different types of audit logs to record user and server-related events as they occur:

1. **Audit Log** which captures all user actions and stores them on the Server's external database (provided by the IT environment).
2. **Server Task Log** which lists the currently running or historical server tasks and long-running actions.

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

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 Audit Log displays the following information:

- User name: specifies the McAfee ePO user name of the account that attempted to take the action. The user name is unavailable for some actions, for example, failed logins.
- Priority: specifies the importance of the action determined by McAfee.
- Action: specifies the action the user attempted to take.
- Details: specifies further information about the action, if available.
- Success: specifies whether the action succeeded.
- Start Time: specifies the time (on the ePO server) the action began.
- Completion Time: specifies the time (on the ePO server) the action was completed.

The Server Task Log List displays the following information:

- Name: specifies the name of the server task or action.
- Start Date: specifies the date and time (on the ePO server) when the task started.
- End Date: specifies the date and time (on the ePO server) when the task ended.
- User name: specifies the McAfee ePO user name of the individual who launched or scheduled the task.

- Status: specifies the current status of the task.
- Source: specifies the source of the server task. For example, a source of "Scheduler" indicates that the server task was the result of a server task scheduled to run automatically, whereas a source of "Server Task" indicates that the task was run manually.
- Duration: specifies how long the task ran, or has been running.

The 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 log entries are stored in the external database.

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

7.8 Protected System Data Transfer

Communications between McAfee Agents and ePO take the form of XML messages. Communications can include policies to implement, properties collected from the managed system, event data gathered by the ENS Client, or tasks to be run on the managed system. The messages are transferred via HTTPS. The TOE protects these transmissions between the ePO and the McAfee Agent from disclosure and modification by encrypting the transmissions under TLS, using AES operating in GCM mode, with 128 bit or 256 bit key sizes (by default the cipher used by ePO and McAfee Agent is DHE-RSA-AES256-GCMSHA384).

In FIPS mode, ePO 5.3.1 uses OpenSSL v1.0.1m with FIPS module v2.0.8 (FIPS 140-2 certificate #1747) for TLS 1.2. McAfee Agent 4.8 uses RSA BSAFE Crypto-C ME v2.1.0 running on Windows Server 2003, Windows Server 2008/R2, Windows Server 2012, Solaris 10 & CentOS 5, 5.5 (FIPS 140-2 certificate #828) to provide cryptographic services for this link. McAfee affirms that the cryptographic modules have been implemented in accordance with their FIPS 140 security policies, and when the TOE is configured in FIPS mode the cryptographic functions operate as intended.

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards	CAVP Cert #
Key Transport	RSA encrypt/decrypt	2048	Allowed in FIPS mode	OpenSSL #1535 BSAFE #203
Symmetric encryption and decryption	Advanced Encryption Standard (AES) (operating in ECB or CBC mode)	256	FIPS 197	OpenSSL #2929 BSAFE #490
Secure Hashing	SHA-384	Not Applicable	FIPS 180-3	OpenSSL #2465 BSAFE #560

Table 30 – Cryptographic Operations Used by the TOE