McAfee

Application Control v5.0, Change Control v5.0, and Integrity Monitor v5.0 with McAfee Agent v4.5 and ePolicy Orchestrator v4.5

Security Target

Evaluation Assurance Level: EAL3+
Document Version: 0.6

Prepared for:

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054

Phone: (800) 847-8766
Email: sales@mcafee.com
http://www.mcafee.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the McAfee Application Control v5.0, Change Control v5.0, and Integrity Monitor v5.0 with McAfee Agent v4.5 and ePolicy Orchestrator v4.5, and will hereafter be referred to as the TOE throughout this document. The TOE is an application control and change control software solution with robust management functionality.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 – ST and TOE References

ST Title	McAfee Application Control v5.0, Change Control v5.0, and Integrity Monitor v5.0 with McAfee Agent v4.5 and ePolicy Orchestrator v4.5 Security Target
ST Version	Version 0.6
ST Author	Corsec Security Inc.
ST Publication Date	2010-12-14
TOE Reference	McAfee ePO Server Extension 5.0.0-160, Solidcore MA Plug-in 5.0.0-6201, ePO Server 4.5.0-6201, McAfee Agent 4.5.0-1499[1]
Keywords	Change Control, Application Control, Integrity Monitor, McAfee, ePolicy Orchestrator, ePO, McAfee Agent, Change Prevention

[1] "Solidcore" represents the Application Control, Change Control, and Integrity Monitor software.

1.3 Product Overview

The Product Overview provides a high level description of the McAfee Application Control v5.0, Change Control v5.0, and Integrity Monitor v5.0 with McAfee Agent v4.5 and ePolicy Orchestrator v4.5 that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

The McAfee Application Control v5.0, Change Control v5.0, and Integrity Monitor v5.0 with McAfee Agent v4.5 and ePolicy Orchestrator v4.5 provides integrity monitoring and change control on servers, desktops, network devices, and databases. It also ensures that only authorized code can run on those managed systems. This functionality is managed through the ePolicy Orchestrator (ePO) management software.

The product consists of four logical components:

- Integrity Monitor (for change monitoring)
- Change Control
- Application Control
- ePO (for management of the Integrity Monitor, Change Control, and Application Control)

These four logical components are implemented via five physical software components:

- Solidifier Service – manages the policy for the Filesystem Driver and interfaces with the CLI and McAfee Agent
- Command Line Interface (CLI) Utility – for local management of the Solidifier Service
- Filesystem Driver (swin.sys) – the portion of the product implemented in the Operating System's (OS) kernel space; the filesystem driver intercepts and analyzes all file system, registry, memory, and other critical reads and writes occurring in the OS and implements the core application control, change control, and integrity monitoring actions
- ePO – for remote management of the Solidifier Service
- McAfee Agent – a plug-in to the Solidifier Service used by ePO

In addition, the product interacts with a third-party database. The database and the five physical software components of the product are shown in Figure 1 below as they are configured in a typical implementation of the product.

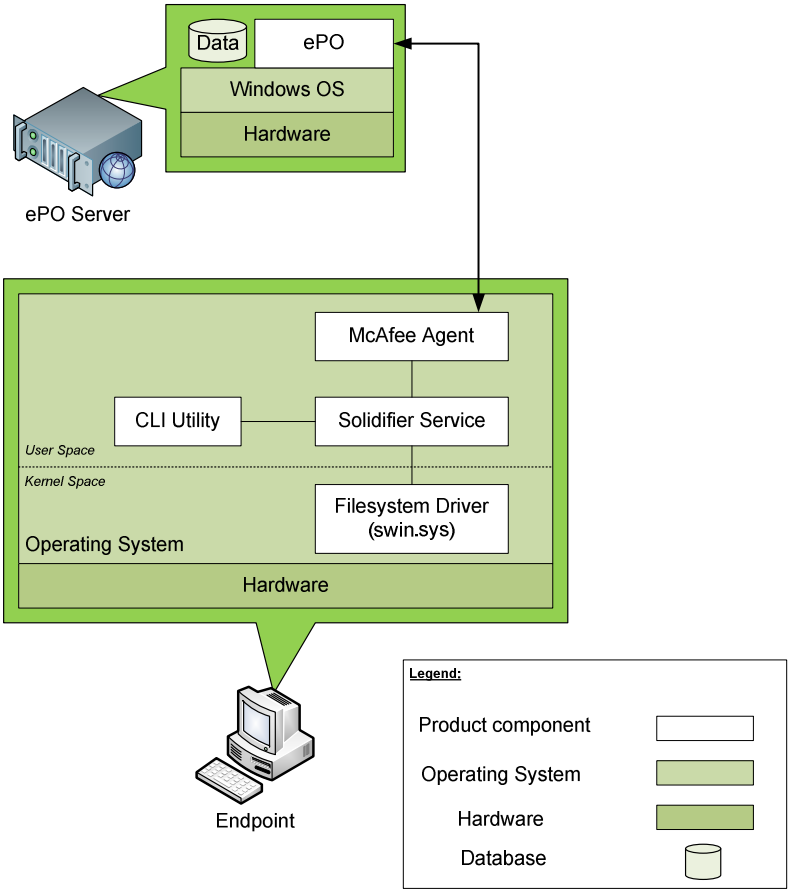

Figure 1 – Software Components of the Product

The following sections describe each of the logical components of the product.

1.3.1 Integrity Monitor

The Solidifier Service contains Integrity Monitor functionality, which monitors change actions happening on the managed system. Integrity Monitor can monitor changes to the following:

- Files and directories
- Windows Registry entries
- Process execution/termination
- User activity (Logon/Logoff)

Integrity Monitor tracks all changes to the files and directories on the managed system. Types of changes monitored on files and directories include:

- Creation
- Modification of contents
- Deletion
- Renaming
- File attribute modification
- Access Control List (ACL) modification
- Owner modification

Integrity Monitor also monitors changes to network file shares, such as Network File Server (NFS) and Client for NFS Services (NFS Client), as well as Common Internet File System (CIFS)/Server Message Block (SMB) for Windows systems. Integrity Monitor also monitors changes to file attributes on Windows systems, such as 'FILE_ATTRIBUTE_ENCRYPTED', and 'FILE_ATTRIBUTE_HIDDEN', etc. Integrity Monitor monitors the start and stop events for process execution, as well. In addition, it monitors the success or failure of user logon and logoff attempts, and other account changes.

For each change made to an object, Integrity Monitor generates a change event. It uses event filters to tailor which change events appear in the event viewer. These filters can be customized by the administrator. Filters can be set on files, directories, registries, process names, file extensions, and user names. Filters match criteria based on file extension, path name, process name, user name, or registry name for change events. Filters can be configured in two different ways:

- Include filters cause events matching the filtering criteria to be reported to the user
- Exclude filters cause events matching the condition to be suppressed and not reported to the user.

The filtering of change events for the purpose of reporting them ensures that only change events the administrator is interested in are recorded. Many change events are program-generated, and may not be of interest to the administrator. Filtering helps reduce the volume of change events being recorded, and thereby reduces the 'noise' on the system. Filter rules are implemented in a predefined order of precedence. For example, filters based on user name will have the highest precedence over all other filter rules.

1.3.2 Change Control

The Solidifier Service also contains Change Policy Enforcement functionality, which prevents specified reads or writes to files and directories on the managed systems. Any addition, removal, or modification of software on the managed system is allowed only when the product is in Update Mode, which also tracks every change action made.

1.3.2.1 Write Protection

Critical files, directories, and volumes can be write-protected using the 'deny-write' feature of Solidifier Services. This renders the specified files as read only. The following operations are controlled by this feature:

- Deletion
- Renaming
- Creation of hard links
- Modifying contents
- Appending
- Truncating
- Changing owner
- Creation of Alternate Data Stream[2] (ADS)

When a directory or volume is specified for write-protection, all files in that directory or volume are added to the write-protected list. These specifications are inherited by sub-directories, as well. In addition to the operations listed above, creation of new files is also denied for directories or volumes listed as write-protected. If any file or directory within a parent directory is write-protected, renaming of the parent directory is also denied. All operations listed above on a write-protected file, directory, or volume are considered unauthorized, and are therefore stopped and an event is generated in the Event Log.

[2] Alternate Data Streams are metadata associated with a file system object, and are also known as "forks".

Critical registry keys can also be protected against change using the 'deny-write' feature. All enforcement rules to control modifications to registry keys can be applied using this feature. Any unauthorized attempts to modify a write-protected registry key will be stopped, and a change event will be generated.

1.3.2.2 Read Protection

Critical files, directories, and volumes can also be read-protected using the 'deny-read' feature of Solidifier Services. This enforces read-protection on specified files, directories, and volumes, and also denies the execution of script files. When a directory or volume is specified for read-protection, all files in that directory or volume are added to the read-protected list. The rules are inherited by sub-directories, as well. All unauthorized attempts to read a read-protected file, directory, or volume are stopped, and an event is generated in the Event Log.

1.3.3 Application Control

The Solidifier Service also contains Application Control functionality, which prevents the execution of unauthorized program code on a managed system. Upon initial configuration, Application Control takes an initial snapshot of the software implemented on a managed system, and creates a whitelist inventory of the program code that exists at that time on the system. The listed program code includes binary executables such as '.exe' and '.dll' files, as well as scripts, such as '.bat', '.cmd', and '.vbs' files. This becomes the list of code that will be allowed to run on the managed system.

The following types of control are enforced on the program code that is resident on the managed system's disk, or executed on the managed system:

- Execution control
- Memory control
- Tamper-proofing

1.3.3.1 Execution Control

Execution control prevents all programs not in the inventory from executing on the managed system. All programs not in the inventory are considered unauthorized, their execution is prevented, and their failure to execute is logged. This enforcement prevents unauthorized programs such as worms, viruses, and spyware, which install themselves, from executing.

1.3.3.2 Memory Control

Memory control protects running processes from malicious attempts to hijack them. Unauthorized code injected into a running process is trapped, halted, and logged. In this fashion, attempts to gain control of a system through buffer overflow and similar exploits are rendered ineffective, and logged.

1.3.3.3 Tamper-proofing

Tamper-proofing prevents intentional and unintentional changes to files that are in the inventory by users or programs.

The Solidifier Service can be put into "Update Mode" in order for software maintenance to be performed. This allows all update actions to be bracketed within an update window. Update actions include addition, removal, or modification of software on the system. It will track every update action and automatically updates the whitelist inventory. This enables new or modified software to run when the managed system returns to normal operation ("Enable Mode").

In addition to real-time prevention of execution of unauthorized code, Application Control also performs reviews of the Event Log and other internal logs of changes to the managed system to identify applications that are attempting to perform updates, or fail to run when they execute. At times these applications should be allowed to update or run, and this information is brought to the attention of the administrator. The administrator can then take the recommended action.

1.3.4 ePolicy Orchestrator

The ePolicy Orchestrator, or ePO, provides a platform for centralized policy management and enforcement of the Application Control and Change Control product on the managed systems. It uses the System Tree to organize managed systems into units for monitoring, assigning policies, scheduling tasks, and taking actions. The System Tree is a hierarchical structure that allows administrators to combine managed systems into groups. Policies can then be applied to groups of managed systems, rather than individually.

ePO allows administrators to manage the targeted systems from a single location through the combination of product policies and client tasks. Policies ensure that the application control, change control, and integrity monitor features are configured correctly. Client tasks are the scheduled actions that run on the managed systems hosting the Solidifier Services. Client tasks are commonly used for product deployment, product functionality, upgrades, and updates.

The ePO software is comprised of several components:

- ePO server
- Registered servers
- Database
- Master repository
- Distributed repositories
- McAfee Agent
- Remote Agent Handlers

Each of these is described in the following sections.

1.3.4.1 ePO Server

This is the center of the managed environment. The ePO server delivers application control, change control, and integrity monitor policies, controls updates, and processes the events for all the managed systems. It includes the following subcomponents:

- Application server – includes the Automatic Response[3] functionality, Registered Servers (see below), and the user interface
- Agent handler – distributes network traffic generated by agent-to-server communications; responsible for communicating policies, tasks, and properties
- Event parser – parses events received from Solidifier Services
- Rogue System Detection[4] (RSD) server and data channel listener

1.3.4.2 Registered Servers

These are used to register the ePO server with other servers. Registered server types include:

- Lightweight Directory Access Protocol (LDAP) server (i.e., Active Directory for Windows systems) – used for Policy Assignment Rules[5] and to enable automatic user account creation[6] (when implemented)

[3] Automatic Responses functionality allows administrators to create rules for responding to events that are specific to the managed business environment, such as sending email notifications or SNMP traps, or creating issues for use with integrated third-party ticketing systems.

[4] Rogue Systems are systems that access the managed network, but are not managed by the ePO server.

[5] Policy Assignment Rules are user-specific policies enforced on managed systems that dictate what the user has access to on or from that managed system. For example, one user might have policy assignment rules that allow unrestricted access to the internet from the managed system. Another user might have heavily restricted access to the internet from a managed system.

[6] User autocreation creates ePO user account records for Active Directory users when they first log on based on Windows authenticated user credentials. Permission sets are dynamically assigned to these users.

- Simple Network Management Protocol (SNMP) server – used for receiving Automatic Responses via SNMP traps
- Ticketing server – examples of use are: to process tickets for issues[7] generated by ePO systems (examples of Ticketing Servers are BMC Remedy Action Request System and Hewlett-Packard Openview Service Desk), or to use existing change tickets to allow updates to protected systems.

1.3.4.3 Database

The database is the central storage component for all data created and used by ePO. The database can be housed on the ePO server, or on a separate server, depending on the specific needs of the organization.

1.3.4.4 Master Repository

The Master Repository is the central location for all McAfee updates and signatures, and it resides on the ePO server. The Master Repository retrieves user-specified updates and signatures from McAfee or from user-defined source sites.

1.3.4.5 Distributed Repository

Distributed Repositories are placed throughout a managed environment to provide managed systems access to receive signatures, product updates, and product installations with minimal bandwidth impact. The Distributed Repositories can take the form of SuperAgent[8], HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), or Universal Naming Convention[9] (UNC) servers.

1.3.4.6 McAfee Agent

The McAfee Agent is a vehicle of information and enforcement between the ePO server and each managed system. The McAfee Agent retrieves updates, ensures task implementation, enforces policies, and forwards events for each managed system. It uses a separate secure channel to transfer data to the ePO server. The McAfee Agent can also be configured as a SuperAgent with the addition of a repository.

1.3.4.7 Remote Agent Handlers

Remote Agent Handlers are servers installed in various network locations to help manage McAfee Agent communication, load balancing, and product updates. Remote Agent Handlers can help administrators manage the needs of large or complex network infrastructures by allowing them more control over agent-server communication.

1.3.5 Product Platforms

Application Control, Change Control, and Integrity Monitor all run on the following platforms:

- Windows 2000
- Windows XP (32- and 64-bit)
- Windows Vista (32- and 64-bit)
- Windows NT Server
- Windows Server 2000
- Windows Server 2003/2008 (32- and 64-bit)
- RedHat Linux 7.2, 8.0, RedHat Enterprise Linux 3.0, 4.0, 5.0
- CentOS 4/5
- Solaris 8, 9, 10
- SuSE EL 9/10
- Oracle EL 5

[7] Issues are created by ePO in response to events generated by Solidifier Services.

[8] A SuperAgent is an agent that can broadcast wake-up calls to other ePO agents located on the same network broadcast segment.

[9] UNC is a standard for identifying servers, printers, and other resources in a network, by assigning share names to them.

- HP/UX 11.0, 11iV1,11iv2
- AIX 5.3 and 5.2
- IBM iSeries (AS/400)
- IBM 4690 OS

In addition, McAfee Application Control also runs on:

- Microsoft Windows CE 6.0
- VMware hypervisors
  - ESX 3.0.x/3i/3.5
  - Virtual Center
  - VMware Server 2.0

McAfee Change Control can control the following databases:

- Oracle (7.3, 8.0, 8i, 9i through 10g)
- MS[10] SQL[11] Server (6.5, 7.0, 2000 through 2005)
- Sybase SQL Server (10.X, 11.0, 11.1, 11.5 through 11.9, 12.X)
- IBM DB2 (5.X to 9.X)

McAfee Change Control can control more than 300 types of network devices, including products from Cisco, HP, 3Com, Nortel, Foundry and NetScreen. ePO Server runs on various Windows platforms.

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The TOE is an application and change control software-only TOE. The TOE includes all the functionality described above in Section 1.3, except those features and functionality listed below in Section 1.5.3. The TOE runs on the platforms described below in Section 1.4.2.

Figure 2 shows the details of the deployment configuration of the TOE:

[10] MS - Microsoft
[11] SQL – Structured Query Language

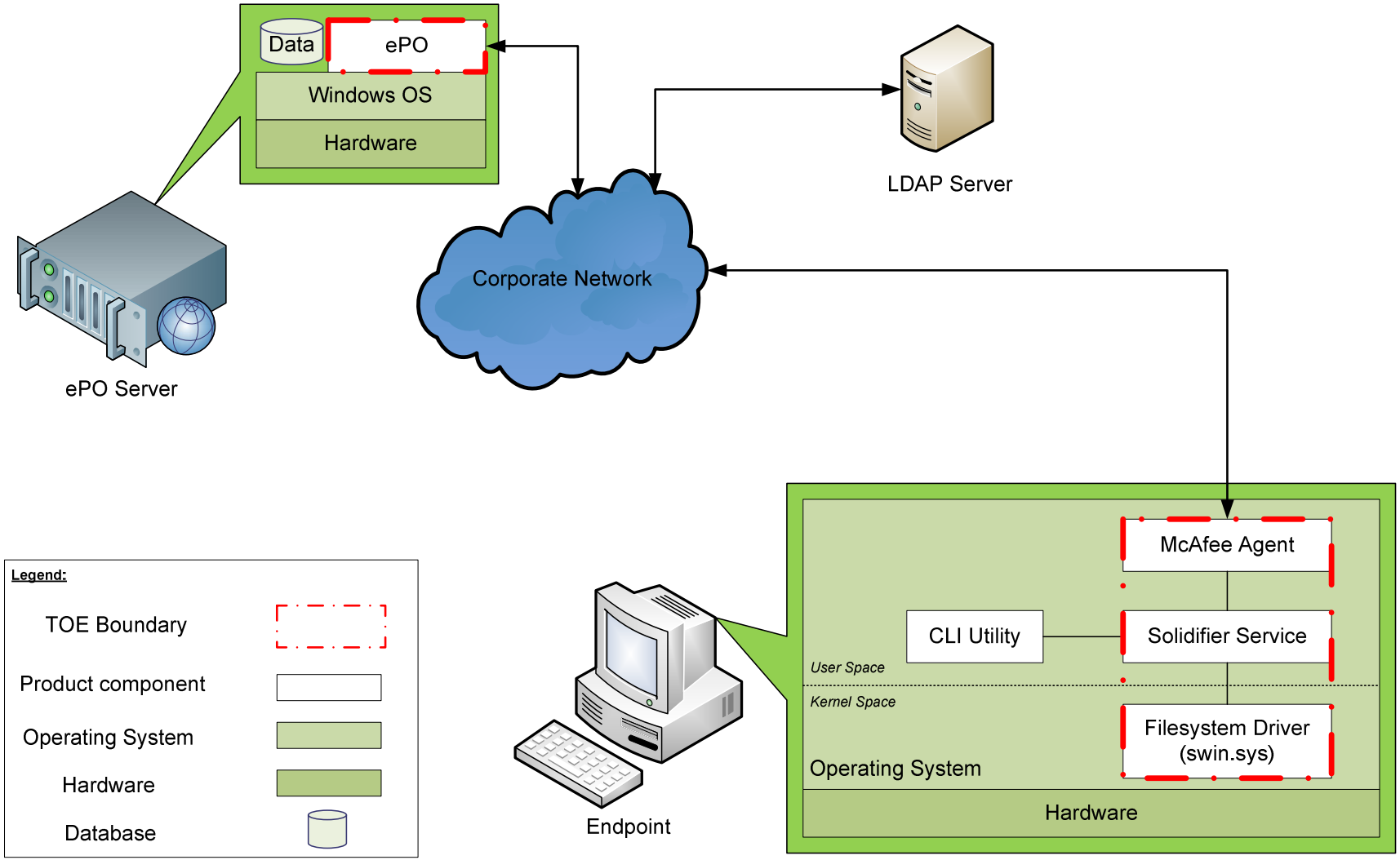

Figure 2 – Deployment Configuration of the TOE

1.4.1 Brief Description of the Components of the TOE

The TOE consists of the following software components:

- Solidifier Service – manages the policy for the Filesystem Driver and interfaces with the CLI and McAfee Agent
- Filesystem Driver (swin.sys) – the portion of the product implemented in the Operating System's (OS) kernel space; the filesystem driver intercepts and analyzes all file system, registry, memory, and other critical reads and writes occurring in the OS and implements the core application control, change control, and integrity monitoring actions
- ePO – for remote management of the Solidifier Service
- McAfee Agent – a plug-in to the Solidifier Service used by ePO

The CLI Utility is excluded from the evaluation, and must be disabled.

The RSA BSAFE Crypto-C Micro Edition v2.0 (FIPS 140-2 certificate number 608) is a third-party product included in the TOE.

1.4.2 TOE Environment

Application Control, Change Control, and Integrity Monitor all run on the following platforms:

- Windows 2000 (32-bit)
- Windows XP (32- and 64-bit)
- Windows Vista (32- and 64-bit)
- Windows NT Server
- Windows Server 2000
- Windows Server 2003/2008 (32- and 64-bit)

ePO runs with MS SQL Server 2005 on Windows Server 2003 and Windows Server 2008 (32- and 64-bit).

The following third-party products are used by the TOE in the CC-evaluated configuration:

- TinyXML-2.5.3
- LDAP Server
- MS SQL Server 2005 database

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.5.1 Physical Scope

Figure 3 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

The TOE is an application control and change control product that runs on a Windows platform compliant to the minimum software and hardware requirements as listed in Table 2. The physical TOE boundary is depicted in Figure 3 below. The essential logical components for the proper operation of the TOE in the evaluated configuration are the TOE software, one of the designated Windows OSs, and an LDAP Server. The general-purpose hardware platforms for the TOE, physical network cables and devices, and servers running required network services (such as Domain Name System – DNS) are the only required physical components for the proper operation of the TOE.

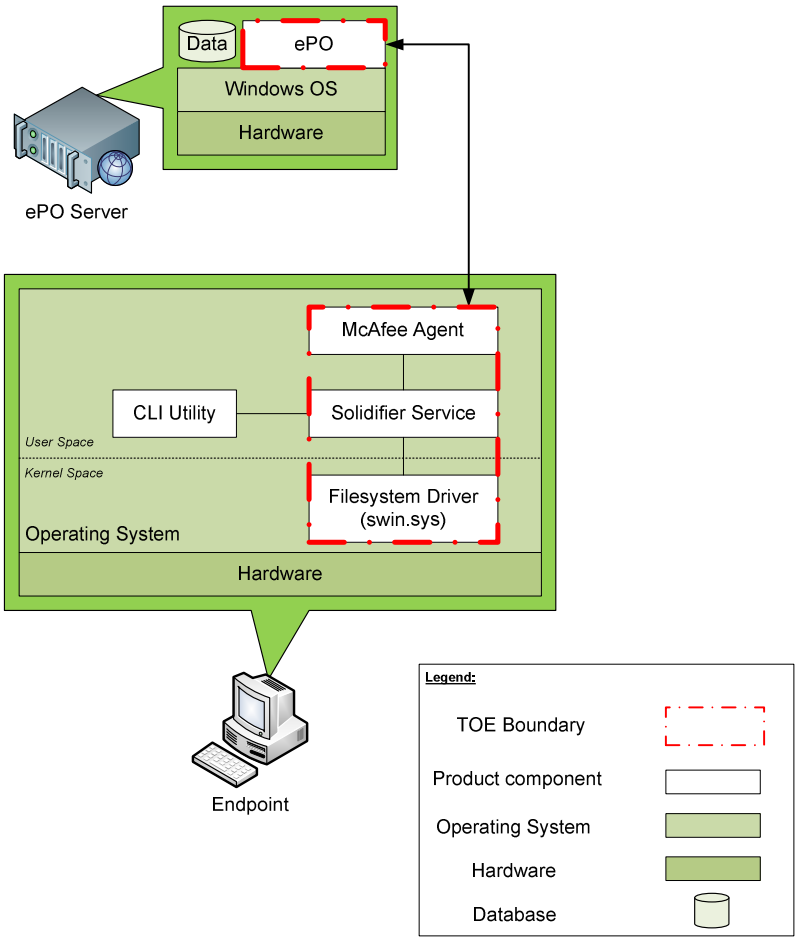

Figure 3 – Physical TOE Boundary

1.5.1.1 TOE Platform Minimum Requirements

Table 2 specifies the minimum system requirements for the proper operation of the TOE.

Table 2 – TOE Platform Minimum Requirements

Component	Minimum System Requirements
Endpoint Workstation	• Single Intel Pentium CPU[12] or higher • 512 MB[13] RAM[14] • 100 MB free disk space • TCP/IP[15] protocol installed • Windows 2000, XP, Vista, Server 2003, or Server 2008 Operating System
ePO Server	• 1 GHz[16] Pentium III-class CPU or higher

[12] CPU – Central Processing Unit
[13] MB – Megabyte
[14] RAM – Random-Access Memory
[15] TCP/IP – Transmission Control Protocol/Internet Protocol
[16] GHz – Gigahertz

Component	Minimum System Requirements
	• 1 GB[17] Physical RAM • 1 GB free disk space • 1024 x 768, 256-color, VGA[18] monitor • 100 MB or higher Network Interface Card • Internet Explorer 7.0 or 8.0 browser or Firefox 3.0 browser • MS SQL Server 2005 database • Windows Server 2003 or Windows Server 2008 Operating System

1.5.1.2 Guidance Documentation

The following guides are required reading and part of the TOE:

- McAfee ePolicy Orchestrator 4.5 Product Guide
- McAfee ePolicy Orchestrator 4.5 Evaluation Guide
- McAfee ePolicy Orchestrator 4.5 Installation Guide
- McAfee ePolicy Orchestrator 4.5 Reporting Guide
- McAfee ePolicy Orchestrator 4.5 Log Files Reference Guide
- Release Notes for McAfee ePolicy Orchestrator 4.5
- McAfee Application Control Quick Start Guide for use with ePO 4.0 and 4.5
- McAfee Change Control Quick Start Guide for use with ePO 4.0 and 4.5
- McAfee Integrity Monitor Quick Start Guide for use with ePO 4.0 and 4.5
- McAfee Solidcore Extension Installation Guide 5.0.0 for use with ePO 4.0 and 4.5
- McAfee Solidcore Extension Product Guide for use with ePO 4.0 and 4.5
- Release Notes for McAfee Solidcore Extension 5.0.0
- Solidcore S3 Control Solidifier User's Guide
- Solidcore S3 Control Solidifier for Windows Runtime Control User's Guide
- Solidcore S3 Control Solidifier for Windows Installation Guide
- Solidcore S3 Control Solidifier for Windows 5.0 Release Notes

1.5.2 Logical Scope

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functions
- McAfee Application and Change Control

1.5.2.1 Security Audit

The TOE generates audit records for all ePO and Solidifier administrator actions. Authorized administrators can view, sort, and filter the audit records. The ePO-generated audit records can be filtered to present only failed actions, or only entries that are within a certain age. Solidifier-generated audit records can be filtered and sorted on the following fields:

- User who performed the action,

[17] GB – Gigabyte
[18] VGA – Video Graphics Array

- target object of the action,
- computer on which the action was performed,
- action timestamp, and
- action type.

1.5.2.2 Cryptographic Support

The TOE protects transmissions between the ePO and the McAfee Agent from disclosure by encrypting the transmissions using the RSA BSAFE Crypto-C Micro Edition v2.0 (FIPS 140-2 certificate number 608).

1.5.2.3 Identification and Authentication

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

Upon successful login, the Global Administrator status and permissions are bound to the session. Those attributes remain fixed for the duration of the session. If the attributes for a logged-in user are changed, those changes will not be bound to a session until the next login by that user.

1.5.2.4 Security Management

The TOE provides administrator support functionality that enables a user to configure and manage TOE components. Management of the TOE is performed via the ePO GUI. Management permissions are defined per-user. The TOE maintains two types of roles: "Global Administrator" and users with limited permissions.

1.5.2.5 Protection of the TSF

The TOE protects transmissions between the ePO and the McAfee Agent from disclosure by securing the transmissions using RSA BSAFE.

1.5.2.6 McAfee Application and Change Control

The TOE provides Application Control, Change Control, and Integrity Monitoring functionality for managed systems. It does this by collecting information about the program code, files, directories, and volumes that are to be protected. Each time a program attempts to execute, or a process or user attempts to modify a protected resource, the TOE analyzes the attempted action, and determines whether it should be allowed or not. It then takes the appropriate action.

1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

Features/Functionality that are not part of the evaluated configuration of the TOE are:

- CLI Utility
- Product Integrity
- Package Control
- AntiDos
- S3 System Controller
- S3 Analytics Server
- Heartbeat Timeout
- Message Exchange Interval
- Secure Signed Update Utility

- Distributed Repositories
- SNMP
- SuperAgents
- ePO local authentication
- Remote Agent Handlers
- Ticketing functionality
- Rogue System Detection
- Open API to Third-party products

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 3 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations from the CEM[19] as of 2010/02/26 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL3 (Augmented with Flaw Remediation (ALC_FLR.2))

[19] CEM – Common Evaluation Methodology

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the Information Technology (IT) assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. The following threats are applicable:

Table 4 – Threats

Name	Description
T.AUTHENTICATE	An authorized user may be unaware of an inadvertent change to TOE data or functions they are authorized to modify.
T.COMPROMISE	An unauthorized user may attempt to disclose, remove, destroy, or compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.PROTECT	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data, or inappropriately change the configuration of the TOE.
T.APP_CHG_CONTROL	An attacker may be able to inappropriately change targeted objects or execute inappropriate software on the managed system without being detected.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no OSPs defined for this Security Target.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 5 – Assumptions

Name	Description
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable to the IT Systems the TOE monitors.
A.TIME	The IT Environment will provide reliable timestamps for the TOE to use.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.PROTECT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
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.DYNAMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 6 – Security Objectives for the TOE

Name	Description
O.AUDIT	The TOE must record audit records for data accesses and use of the TOE functions on the management system.
O.ACCESS	The TOE must allow authorized users to access only authorized TOE functions and data.
O.AUDIT_REVIEW	The TOE must provide authorized administrators with the ability to review, order, and filter the audit trail.
O.IDENTIFY	The TOE must be able to identify users prior to allowing access to TOE administrative functions and data.
O.EADMIN	The TOE must include a set of functions that allow efficient management of its functions and data.
O.PROTECT	The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.
O.COLLECT	The TOE shall collect a list of objects that are to be protected and an inventory of allowable program code for the managed systems.
O.ANALYZE	The TOE must apply analytical processes and information to derive conclusions about allowed and disallowed accesses to objects.
O.REACT	The TOE shall take appropriate action on all allowed and disallowed accesses to objects.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 7 – IT Security Objectives

Name	Description
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.
OE.INTEROP	The TOE is interoperable with the managed systems it monitors.
OE.AUTHENTICATE	The TOE environment must authenticate all users prior to allowing them to access TOE data and functions.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 8 – Non-IT Security Objectives

Name	Description
NOE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.
NOE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
NOE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 9 identifies all extended SFRs implemented by the TOE

Table 9 – Extended TOE Security Functional Requirements

Name	Description
EXT_MAC_SDC.1	Application and Change Control Data Collection
EXT_MAC_ANL.1	Application and Change Control Analysis
EXT_MAC_RCT.1	Application and Change Control React

5.1.1 Class EXT_MAC: McAfee Application and Change Control

Application and Change Control functions involve enforcement of restrictions on execution of applications on the targeted system, and on modification of files on the targeted system. The EXT_MAC: McAfee Application and Change Control class was modeled after the CC FAU: Security Audit class.

The extended family EXT_MAC_SDC: Application and Change Control Data Collection was modeled after the CC family FAU_GEN: Security Audit Data Generation. The extended family EXT_MAC_ANL: Application and Change Control Analysis was modeled after the family FAU_SAA: Potential Violation Analysis. The extended family EXT_MAC_RCT: Application and Change Control React was modeled after the family FAU_ARP: Security Alarms.

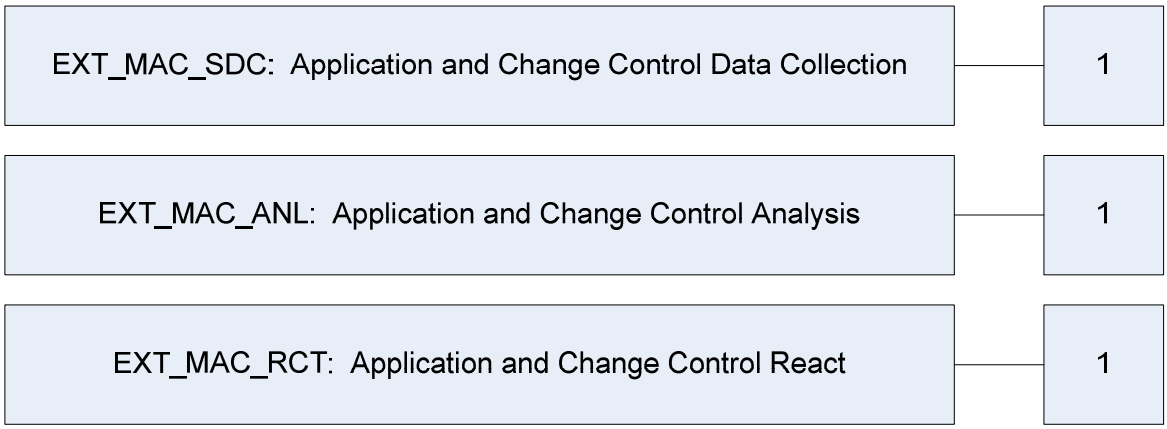

Figure 4 – EXT_MAC: McAfee Application and Change Control Class Decomposition

5.1.1.1 Application and Change Control Data Collection (EXT_MAC_SDC)

Family Behaviour

This family defines the requirements for creating a baseline snapshot of the targeted system for use in determining which applications will be allowed to execute on the system, as well as identifying changes to files, directories, network shares, registry keys, and user accounts. This family enumerates the types of program code that shall be collected by the TOE Security Function (TSF), and identifies what type of control will be enforced on the executable code. This family also determines which change events will be prevented, and which change events will be monitored and reported.

Component Leveling

Figure 5 – Application and Change Control Data Collection family decomposition

EXT_MAC_SDC.1 Application and change control data collection, specifies the list of executable code that shall be allowed to run on the targeted system, as well as identifies changes to files, directories, network shares, registry keys, and user accounts.

Management: EXT_MAC_SDC.1

- There are no management activities foreseen.

Audit: EXT_MAC_SDC.1

- There are no auditable events foreseen.

EXT_MAC_SDC.1 Application and change control data collection

Hierarchical to: No other components

Dependencies: No dependencies

EXT_MAC_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s): [assignment: lists of program code allowed to execute, and changes to files, directories, network shares, registry keys, and user accounts].

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

- ***[assignment: list of data collected].***

5.1.1.2 Application and Change Control Analysis (EXT_MAC_ANL)

Family Behaviour

This family defines the analysis the TOE performs on the collected application and change control data. This family enumerates the types of program code that shall be collected by the TSF, and identifies what type of control will be enforced on the executable code. This family also determines which changes are to be prevented, and which are to be monitored and reported.

Component Leveling

Figure 6 – Application and Change Control Analysis family decomposition

EXT_MAC_ANL.1 Application and change control analysis, specifies the list of analyses the TOE will perform on the collected application data.

Management: EXT_MAC_ANL.1

- Maintenance of the analysis functions by (adding, modifying, deletion) of policies from the set of policies.

Audit: EXT_MAC_ANL.1

- Minimal: Enabling and disabling of any of the analysis mechanisms.

EXT_MAC_ANL.1 **Application and change control analysis**
Hierarchical to: No other components

Dependencies: EXT_MAC_SDC.1

EXT_MAC_ANL.1.1 The System shall perform the following analysis function(s) on all application data collected:

a) [assignment: analytical functions.]

5.1.1.3 Application and Change Control React (EXT_MAC_RCT)

Family Behaviour

This family defines the actions to be taken by the TOE for each analytical event performed on the application and change control data.

Component Leveling

Figure 7 – Application and Change Control React family decomposition

EXT_MAC_RCT.1 Application and change control react, specifies the list of actions that shall be taken for each analytical result obtained against the collected application and change control data.

Management: EXT_MAC_RCT.1

- The management (addition, removal, or modification) of actions.

Audit: EXT_MAC_RCT.1

- Minimal: Actions taken due to application analysis requirements.

EXT_MAC_RCT.1	**Application and change control react**
Hierarchical to:	No other components
Dependencies:	EXT_MAC_SDC.1 EXT_MAC_ANL.1

EXT_MAC_RCT.1.1 The System shall take the following actions [assignment: appropriate actions] when an application analysis requires it.

5.2 Extended TOE Security Assurance Components

This section specifies the extended SARs for the TOE. There are no extended SARs defined for this ST.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

6.1.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 10 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 10 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FAU_SAR.2	Restricted audit review				
FAU_SAR.3	Selectable audit review		✓		
FCS_COP.1	Cryptographic operation		✓	✓	
FIA_ATD.1	User attribute definition		✓		
FIA_UID.2	User identification before any action				
FIA_USB.1	User-subject binding		✓		
FMT_MTD.1	Management of TSF data	✓	✓	✓	
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_ITT.1	Basic internal TSF data transfer protection	✓			
EXT_MAC_SD	Application and change control data collection		✓		

Name	Description	S	A	R	I
C.1					
EXT_MAC_ANL.1	Application and change control analysis		✓		
EXT_MAC_RCT.1	Application and change control react		✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation
Hierarchical to: No other components.
FAU_GEN.1.1
The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events, for the [not specified] level of audit; and
c) [*all Solidifier and ePO administrator actions*].
FAU_GEN.1.2
The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit-relevant information*].
Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review
Hierarchical to: No other components.
FAU_SAR.1.1
The TSF shall provide [*authorised users with Global Administrator status or the View Audit Log permission*] 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.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.2 Restricted audit review
Hierarchical to: No other components.
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.
Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3 Selectable audit review
Hierarchical to: No other components.
FAU_SAR.3.1
The TSF shall provide the ability to apply [*sorting and filtering*] of audit data based on [*the fields listed in Table 11 below*].

Table 11 – Selectable audit review fields

TOE Component	Field	Filter/Sort
ePO	Action	Sort

TOE Component	Field	Filter/Sort
	Completion time	Filter, Sort
	Details	Sort
	Priority	Sort
	Start Time	Filter, Sort
	Success	Filter, Sort
	User Name	Sort
Solidifier	Who performed the action	Filter, Sort
	Target object of the action	Filter, Sort
	Computer on which action was performed	Filter, Sort
	Action timestamp	Filter, Sort
	Action type	Filter, Sort

Dependencies: FAU_SAR.1 Audit review

6.2.2 Class FCS: Cryptographic Support

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.
FCS_COP.1.1

The TSF shall perform [*list of cryptographic operations* – **see Table 12 below**] in accordance with a specified cryptographic algorithm [*cryptographic algorithm* – **see Table 12 below**] and cryptographic key sizes [*cryptographic key sizes* – **see Table 12 below**] that meet the following: [*list of standards* – **see Table 12 below**].

Table 12 - Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Digital signature verification	DSA	1024	FIPS 186-2 (certificate #143)
Key Transport	RSA encrypt/decrypt	1024, 2048	Allowed in FIPS mode
Symmetric encryption and decryption	Advanced Encryption Standard (AES) (CBC[20], mode)	128, 256	FIPS 197 (certificate #303)
	Triple-Data Encryption Standard (3DES[21]) (CBC mode)	2-key and 3-key	FIPS 46-3 (certificate #378)
Random Number Generation	FIPS 186-2 PRNG	Not Applicable	FIPS 186-2 Appendix 3.1 with Change Notice 1 (certificate #130)
Session Authentication	Keyed-Hash Message Authentication Code (HMAC) with Secure Hash Algorithm 1 (SHA -1)	Not Applicable	FIPS 198 (certificate #113)
Secure Hashing	SHA-1	Not Applicable	FIPS 180-3 (certificate #380)

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

[20] CBC – Cipher Block Chaining
[21] 3DES – Triple Data Encryption Standard

6.2.3 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition
Hierarchical to: No other components.
FIA_ATD.1.1
The TSF shall maintain the following list of security attributes belonging to individual users: [
a) *ePO User name;*
b) *Enabled or disabled;*
c) *Authentication configuration;*
d) *Global Administrator status;*
e) *Permission sets*].
Dependencies: No dependencies

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
FIA_UID.2.1
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: No dependencies

FIA_USB.1: User-subject binding
Hierarchical to: No other components
FIA_USB.1.1:
The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [
a) *Global Administrator status; and*
b) *permissions*].
FIA_USB.1.2:
The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [*user security attributes are bound upon successful login with a valid ePO User Name and upon each consecutive action that causes the GUI to refresh*].
FIA_USB.1.3:
The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [*user security attributes do not change until a GUI refresh occurs*].
Dependencies: FIA_ATD.1 User Attribute Definition

6.2.4 Class FMT: Security Management

FMT_MTD.1 Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1

The TSF shall restrict the ability to [query, modify, delete, *create, enable, disable, import, export, make public, and use* **as specified in Table 13 below**] the [*TSF data listed in Table 13 below*] to [*a Global administrator or a user with the permissions identified in Table 13 below*].

Table 13 – TSF Data Access Permissions

TSF Data	Associated Permission	Operations Permitted
Dashboards	Use public dashboards	Use public dashboards
	Use public dashboards; create and edit personal dashboards	Use public dashboards; create and modify personal dashboards
	Use public dashboards; create and edit personal dashboards	Use public dashboards; create, delete, and modify personal dashboards; make personal dashboards public
Contacts	Create and edit contacts	Query, create, delete, and modify
	Use contacts	Use
Application and Change Control Log Files	Configure the event cache size; Configure the log file location path; Configure the size of the log file; Configure the number of log files	Modify
ePO User Accounts	n/a (only allowed by a Global Administrator)	Query, create, delete, and modify
Event Filtering	n/a (only allowed by a Global Administrator)	Query and modify
Global Administrator Status	n/a (only allowed by a Global Administrator)	Query and modify
Groups	View "System Tree" tab	Query
	View "System Tree" tab along with Edit System Tree groups and systems	Query, create, delete, and modify
Notification Rules	View notification rules and Notification Log	Query
	Create and edit notification rules; view Notification Log	Query, create, delete, and modify

TSF Data	Associated Permission	Operations Permitted
	Create and edit notification rules; view and purge Notification Log; create and edit SNMP servers and external commands	Query, create, delete, and modify
Permission Set	n/a (only allowed by a Global Administrator)	Query, create, delete, modify, and assign (to a user) permissions
Application Control Rules	Create, edit, remove, and list application control rules	Query, create, delete, and modify
Change Control Rules	Create, edit, remove, and list write-protect rules; Create, edit, remove, and list read-protect rules	Query, create, delete, and modify
Integrity Monitor Rules	Create, edit, remove, and list integrity monitor rules	Query, create, delete, and modify
System Features	Enable, disable or list system features	Enable and disable
Advanced Configurations	Configure the standard event delivery destination; Configure process execution monitoring; Manage mass deployments and system upgrades (via export and import of configuration items)	Modify, export, import
Queries	Use public queries	Query and use public queries
	Use public queries; create and edit personal queries	Query and use public queries; create and modify personal queries
	Edit public queries; create and edit personal queries; make personal queries public	Query, delete, modify, and use public queries; create, delete, and modify (including make public) personal queries
Server Settings	n/a (only allowed by a Global Administrator)	Query and modify
System Information	Create and edit systems	Query, create, delete, and modify
System Tree	View System Tree	Query
Tags	Create and edit tags and tag criteria (all tags); Create and edit tags (tags w/o criteria only)	Query, create, delete, and modify

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [*management of TSF data*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*Global Administrator and Users with Limited Permissions*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.5 Class FPT: Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

FPT_ITT.1.1

The TSF shall protect TSF data from [disclosure] when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies

6.2.6 Class EXT_MAC: McAfee Application and Change Control

EXT_MAC_SDC.1 Application and change control data collection
Hierarchical to: No other components
EXT_MAC_SDC.1.1
The System shall be able to collect the following information from the targeted IT System resource(s):
[
For application control:
- *a. A whitelist inventory of program code, including binary executables and scripts to be used to determine which code should be allowed to execute;*
- *b. Events indicating prevented unauthorized executions of program code;*
- *c. Events indicating prevented attempts to modify files;*

For change control:
- *d. A list of critical files, directories, and volumes that are to be write-protected;*
- *e. A list of all critical files, directories and volumes that are to be read-protected;*
- *f. A list of all critical registry keys that are to be write-protected;*

For integrity monitoring:
- *g. Events indicating the following actions on files, directories, network shares, file attributes: creation, modification of contents, deletion, renaming, file attribute modification, ACL modification, owner modification;*
- *h. Events indicating the start and stop events for process execution;*
- *i. Events indicating the success or failure of user logon or logoff attempts and user account management activities such as user account creation, user account deletion, user account modification (account locked, account unlocked, account enabled, account disabled, and password changed);*

]

EXT_MAC_SDC.1.2
At a minimum, the System shall collect and record the following information:
[
- *a) For application control:*
  The program code identifier;
- *b) For change control:*
  The name of the file, directory, volume, or key to be protected;
- *c) For integrity monitoring:*
  User name, time, event id, action, subject acted upon, and the name of the program making the change.

]
Dependencies: No dependencies

EXT_MAC_ANL.1 Application and change control analysis
Hierarchical to: No other components
EXT_MAC_ANL.1.1
The System shall perform the following analysis function(s) on all application data collected:
[
- *a) For application control:*
  - *a. Compare the identifier of any program attempting to execute with the whitelist inventory;*
  - *b. Analyze the events in the Event Log and internal logs to identify legitimate applications that were prevented from performing updates;*

c. *Analyze the events in the Event Log and internal logs to identify legitimate applications that were prevented from modifying files;*
d. *Analyze the events in the Event Log and internal logs to identify legitimate applications that were preventing from executing;*

b) For change control:
a. *Compare the name of any file that a process is attempting to delete, rename, create hard links for, modify contents of, append data to, truncate, change owner of, and create Alternate Data Stream for with those listed as write-protected;*
b. *Compare the name of any file that a process is attempting to read, or execute script files against, with those listed as read-protected;*
c. *Compare the identifier for any registry key that a process is attempting to modify with those listed as write-protected;*

c) For integrity monitoring:
d. *Compare the change events to the include filters and exclude filters defined for integrity monitoring.*

]
Dependencies: **EXT_MAC_SDC.1**

EXT_MAC_RCT.1 Application and change control react
Hierarchical to: **No other components**
EXT_MAC_RCT.1.1
The System shall take the following actions
[

a) For application control:
a. *Allow execution of any program listed on the whitelist inventory;*
b. *Provide recommendation to administrators to execute the 'sadmin diag' command to allow legitimate applications that were prevented from performing updates to perform those updates;*
c. *Provide recommendation to administrators to execute the 'sadmin diag' command to allow legitimate applications that were prevented from modifying files to modify those files;*
d. *Provide recommendation to administrators to execute the 'sadmin diag' command to allow legitimate applications that were preventing from executing to execute;*

b) For change control:
a. *Prevent deletion of, renaming of, creation of hard links for, modification of contents of, appending data to, truncation of, change of owner for, and creation of Alternate Data Stream for any file listed as write-protected;*
b. *Deny reading of data in, and execution of script files against any file listed as read-protected;*
c. *Prevent modification of registry keys listed as write-protected;*

c) For change monitoring:
a. *Write the filtered change events to the change logs for viewing by administrators.*

]
when an application analysis requires it.
Dependencies: **EXT_MAC_SDC.1**
EXT_MAC_ANL.1

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL3 augmented with ALC_FLR.2. Table 14 – Assurance Requirements summarizes the requirements.

Table 14 – Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM[22] coverage
	ALC_DEL.1 Delivery Procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_FLR.2 Flaw Reporting procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

[22] CM – Configuration Management

7 TOE Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 15 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SAR.3	Selectable audit review
Cryptographic Support	FCS_COP.1	Cryptographic operation
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UID.2	User identification before any action
	FIA_USB.1	User-subject binding
Security Management	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of TOE Security Functions	FPT_ITT.1	Basic internal TSF data transfer protection
McAfee Application and Change Control	EXT_MAC_SDC.1	Application and change control data collection
	EXT_MAC_ANL.1	Application and change control analysis
	EXT_MAC_RCT.1	Application and change control react

7.1.1 Security Audit

The TOE generates audit records for all ePO and Solidifier administrator actions. Authorized administrators can view, sort, and filter the audit records. The ePO-generated audit records can be filtered to present only failed actions, or only entries that are within a certain age. Solidifier-generated audit records can be filtered and sorted on the following fields:

- User who performed the action,
- target object of the action,
- computer on which the action was performed,
- action timestamp, and
- action type.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3.

7.1.2 Cryptographic Support

The TOE protects transmissions between the ePO and the McAfee Agent from disclosure by encrypting the transmissions using the RSA BSAFE Crypto-C Micro Edition v2.0 (FIPS 140-2 certificate number 608).

7.1.3 Identification and Authentication

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

The password entered by the user is passed to the Windows operating system for verification; therefore, the TOE IT Environment handles the authentication of users. If it is validated, the TOE grants access to authorized TOE functionality. If the password is not validated, the login GUI is redisplayed to the user.

For each defined user account, the following information is configured:

- User name
- Enabled or disabled
- Whether authentication for this user is to be performed by ePO or Windows (the evaluated configuration requires Windows authentication for all users)
- Global Administrator status
- Permission sets granted to the user

Upon successful login and each consecutive action taken that causes a GUI refresh, the Global Administrator status and permissions are bound. Those attributes remain fixed until an action causes the GUI to refresh. If the attributes for a logged-in user are changed, those changes will not be bound to a subject until the next GUI action by that user.

TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_UID.2, FIA_USB.1.

7.1.4 Security Management

The TOE provides administrator support functionality that enables a user to configure and manage TOE components. Management of the TOE is performed via the ePO GUI. Management permissions are defined per-user.

The TOE provides functionality to manage the following TSF data:

- Dashboards
- Contacts
- Email Servers
- Application and Change Control Log Files
- ePO User Accounts
- Event Filtering
- Global Administrator Status
- Groups
- Notification Rules
- Permission Sets

- Application Control Rules
- Change Control Rules
- Integrity Monitor Rules
- System Features
- Advanced Configurations
- Queries
- Server Settings
- System Information
- System Tree
- Tags.

The TOE maintains two types of roles: "Global Administrator" and users with limited permissions. 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 any users who are not Global Administrators. Global Administrators are granted all permissions. Each user authorized for login to ePO must be defined within ePO. Only Global Administrators may perform ePO user account management functions (create, view, modify, and delete).

One or more permission sets may be associated with an account. Global Administrators are granted all permissions. Permisions exclusive to Global Administrators (that are not granted via permission sets) include:

- Change server settings
- Create and delete user accounts
- Create, delete, and assign permission sets
- Limit events that are stored in ePO databases.

TOE Security Functional Requirements Satisfied: FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

7.1.5 Protection of the TSF

The TOE protects transmissions between the ePO and the McAfee Agent from disclosure by securing the transmissions using RSA BSAFE Crypto-C Micro Edition v2.0 (FIPS 140-2 certificate number 608).

TOE Security Functional Requirements Satisfied: FPT_ITT.1.

7.1.6 McAfee Application and Change Control

The TOE provides Application Control, Change Control, and Integrity Monitoring functionality for managed systems. It does this by collecting information about the program code, files, directories, and volumes that are to be protected. Each time a program attempts to execute, or a process or user attempts to modify a protected resource, the TOE analyzes the attempted action, and determines whether it should be allowed or not. It then takes the appropriate action.

7.1.6.1 Application Control

Application Control functionality prevents the execution of unauthorized program code on a managed system. Upon initial configuration, Application Control takes an initial snapshot of the software implemented on a managed system, and creates a whitelist inventory of the program code that exists at that time on the system. The listed program code includes binary executables such as '.exe' and '.dll' files, as well as scripts, such as '.bat', '.cmd', and '.vbs' files. This becomes the list of code that will be allowed to run on the managed system.

Whenever a program or process attempts to execute, the TOE compares the program identifier with the list of identifiers collected in the whitelist inventory at initial configuration. If the program is listed on the whitelist, the TOE allows the program to execute. If it is not listed, the TOE stops the program from executing.

In addition, the TOE analyzes the events generated by the TOE and stored in the Event Log to identify legitimate applications that were prevented from performing updates, modifying files, or executing. If legitimate programs are identified, the TOE provides recommendations to the administrator on how to allow those programs to execute in the future.

7.1.6.2 Change Control

Change Control functionality prevents specified reads or writes to files and directories on the managed systems. Critical files, directories, and volumes can be write-protected using the 'deny-write' feature of Solidifier Services. This renders the specified files as read only. Critical files, directories, and volumes can also be read-protected using the 'deny-read' feature of Solidifier Services. This enforces read-protection on specified files, directories, and volumes, and also denies the execution of script files.

The TOE maintains a list of critical files, directories, volumes, and registry keys that are to be write-protected. If a process attempts to delete, rename, create hard links for, modify the contents of, append data to, truncate, change the owner of, or create Alternate Data Streams for a file that is listed as write-protected, the TOE will prevent the action from taking place.

The TOE also maintains a list of all critical files, directories, and volumes that are to be read-protected. If a process attempts to read files or execute script files against a file that is listed as read-protected, the TOE will prevent the action from taking place.

7.1.6.3 Integrity Monitor

Integrity Monitor functionality tracks change actions happening on the managed system. The TOE collects events indicating change actions on files, directories, network shares, and file attributes. It also collects events that indicate the starting and stopping of processes, and the success or failure of user logon or logoff attempts and user account management activities. The TOE then compares these events with the include and exclude filters defined by the administrator. If there is a match, then the TOE writes the specified events to the change logs for viewing by administrators.

TOE Security Functional Requirements Satisfied: EXT_MAC_SDC.1, EXT_MAC_ANL.1, EXT_MAC_RCT.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target extends Part 2 and conforms to Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1 revision 3.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, polices, and assumptions to the security objectives is complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 16 displays the mapping of threats to objectives.

Table 16 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.AUTHENTICATE An authorized user may be unaware of an inadvertent change to TOE data or functions they are authorized to modify.	O.AUDIT The TOE must record audit records for data accesses and use of the TOE functions on the management system.	O.AUDIT counters this threat by ensuring that the TOE tracks all management actions taken against the TOE.
	O.AUDIT_REVIEW The TOE must provide authorized administrators with the ability to review, order, and filter the audit trail.	O.AUDIT_REVIEW counters this threat by ensuring that administrators can review the audited changes to the TOE configuration.
	O.IDENTIFY The TOE must be able to identify users prior to allowing access to TOE administrative functions and data.	O.IDENTIFY counters this threat by ensuring that only identified users can access the TOE administrative functions and data.
	OE.AUTHENTICATE The TOE environment must authenticate all users prior to allowing them to access TOE data and functions.	OE.AUTHENTICATE counters this threat by ensuring that the TOE Environment allows only authorized users access to the TOE functions and data.
T.COMPROMISE An unauthorized user may attempt to disclose, remove, destroy, or compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.	O.ACCESS The TOE must allow authorized users to access only authorized TOE functions and data.	O.ACCESS counters this threat by ensuring that the TOE allows only authorized users access to the TOE functions and data.
	O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	O.PROTECT counters this threat by ensuring that the TOE protects the TOE data from unauthorized access.
T.PROTECT	O.ACCESS	O.ACCESS counters this threat by ensuring

Threats	Objectives	Rationale
An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data, or inappropriately change the configuration of the TOE.	The TOE must allow authorized users to access only authorized TOE functions and data.	that the TOE protects the TOE functions and data from unauthorized access.
	O.EADMIN The TOE must include a set of functions that allow efficient management of its functions and data.	O.EADMIN counters this threat by ensuring that the TOE provides a means to effectively manage the TOE.
	O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	O.PROTECT counters this threat by ensuring that the TOE protects itself from access by unauthorized users.
T.APP_CHG_CONTROL An attacker may be able to inappropriately change targeted objects or execute inappropriate software on the managed system without being detected.	O.COLLECT The TOE shall collect a list of objects that are to be protected and an inventory of allowable program code for the managed systems.	O.COLLECT counters this threat by ensuring that the TOE collects information about the managed systems to be used to determine whether given processes or changes should be allowed or disallowed.
	O.ANALYZE The TOE must apply analytical processes and information to derive conclusions about allowed and disallowed accesses to objects.	O.ANALYZE counters this threat by ensuring that the TOE applies analytical processes and information to derive conclusions about allowed and disallowed actions on the managed systems.
	O.REACT The TOE shall take appropriate action on all allowed and disallowed accesses to objects.	O.REACT counters this threat by ensuring that the TOE takes actions to prevent or allow changes or program executions on the managed systems.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

There are no Policies defined for this Security Target. Therefore,there are no Security Objectives relating to policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 17 – Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.	OE.INTEROP The TOE is interoperable with the managed systems it monitors.	OE.INTEROP upholds this assumption by ensuring that the TOE can interoperate with the managed systems, thereby having access to all the system data is needs to

Assumptions	Objectives	Rationale
		perform its functions.
A.ASCOPE The TOE is appropriately scalable to the IT Systems the TOE monitors.	OE.INTEROP The TOE is interoperable with the managed systems it monitors.	OE.INTEROP upholds this assumption by ensuring that the TOE successfully scales to the managed systems, thereby gaining access to all the system data is needs to perform its functions.
A.TIME The IT Environment will provide reliable timestamps for the TOE to use.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME upholds the assumption that the environment provides reliable timestamps to the TOE.
A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	NOE.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.	NOE.PHYSICAL upholds this assumption by ensuring that physical security is provided within the TOE environment to provide appropriate protection to the network resources.
A.PROTECT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.	NOE.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.	NOE.PHYSICAL upholds this assumption by ensuring that the TOE environment provides protection from external interference or tampering.
A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	NOE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.	OE.MANAGE satisfies the assumption that competent individuals are assigned to manage the TOE and the TSF.
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.	NOE.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.	NOE.INSTALL upholds this assumption by ensuring that personnel installing, managing, and operating the TOE do so efficiently and correctly.
	NOE.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.	NOE.PHYSICAL upholds this assumption by ensuring that the users who install, manage, and operate the TOE do so in a manner that protects it from physical access by unauthorized personnel.
	NOE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.	OE.MANAGE satisfies the assumption that the users who manage the TOE are non-hostile, appropriately trained and follow all guidance.
A.DYNAMIC The TOE will be managed in a manner that allows it to appropriately address changes in	OE.INTEROP The TOE is interoperable with the managed systems it monitors.	OE.INTEROP upholds this assumption by ensuring that the TOE interoperates with the managed systems, thereby allowing them to be managed by the TOE.

Assumptions	Objectives	Rationale
the IT System the TOE monitors.	NOE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.	NOE.PERSON upholds this assumption by ensuring that only properly trained personnel are allowed to operate the TOE.

Every Assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

A class of EXT_MAC requirements was created to specifically address the Application Control, Change Control, and Integrity Monitoring functionality of the TOE. The FAU: Security Audit class was used as a model for creating these requirements. The purpose of this class of requirements is to define the security functionality provided by the Solidifier Service of the TOE. There are no existing CC SFRs that can be used to appropriately describe this Solidifier functionality, so the extended components were created with wording that adequately captures the Solidifier functionality being claimed. These requirements have no dependencies outside their own class since the stated requirements embody all the necessary security functions. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

8.4 Rationale for Extended TOE Security Assurance Requirements

No extended TOE Security Assurance Requirements were defined for this Security Target.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 18 – Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT The TOE must record audit records for data accesses and use of the TOE functions on the management system.	FAU_GEN.1 Audit data generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security-related events, including relevant details about the event.
O.ACCESS	FAU_GEN.1	The requirement meets this objective by

Objective	Requirements Addressing the Objective	Rationale
The TOE must allow authorized users to access only authorized TOE functions and data.	Audit data generation	providing audits of all management actions taken on the TOE for review by administrators.
	FAU_SAR.1 Audit review	The requirement meets this objective by providing the capability to review the audit trail of all management actions taken on the TOE.
	FAU_SAR.2 Restricted audit review	The requirement meets the objective by ensuring that the TOE allows only authorized administrators the ability to review the audit records.
	FAU_SAR.3 Selectable audit review	The requirement meets the objective by ensuring that the TOE provides only authorized administrators the ability to review, order, and filter the audit trail.
	FIA_ATD.1 User attribute definition	The requirement meets the objective by ensuring that the TOE maintains a list of security attributes belonging to individual users.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the TOE identifies all users prior to allowing them access to any TOE functions or data.
	FIA_USB.1 User-subject binding	The requirement meets the objective by ensuring that the TOE binds a user's security attributes to the user's session.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that only authorized users are allowed access to TSF data.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that only authorized administrators are allowed access to TSF functions and data.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that only users with authorized administrative roles are allowed access to TSF functions and data.
O.AUDIT_REVIEW The TOE must provide authorized administrators with the ability to review, order, and filter the audit trail.	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides the ability to review, order, and filter the audit trail.
	FAU_SAR.2 Restricted audit review	The requirement meets the objective by ensuring that the TOE allows authorized administrators the ability to review the audit records.
	FAU_SAR.3	The requirement meets the objective by

Objective	Requirements Addressing the Objective	Rationale
	Selectable audit review	ensuring that the TOE provides authorized administrators the ability to review, order, and filter the audit trail.
O.IDENTIFY The TOE must be able to identify users prior to allowing access to TOE administrative functions and data.	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the TOE identifies all users prior to allowing them access to any TOE functions or data.
O.EADMIN The TOE must include a set of functions that allow efficient management of its functions and data.	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that the TOE provides a means to effectively manage the TOE functions and data.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE provides administrative roles to facilitate the management of the TSF.
O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	FCS_COP.1 Cryptographic operation	The requirement meets the objective by ensuring that the TOE protects TSF data from disclosure when it is transmitted between separate parts of the TOE.
	FPT_ITT.1 Basic internal TSF data transfer protection	The requirement meets the objective by ensuring that the TOE protects TSF data from disclosure when it is transmitted between separate parts of the TOE.
O.COLLECT The TOE shall collect a list of objects that are to be protected and an inventory of allowable program code for the managed systems.	EXT_MAC_SDC.1 Application and change control data collection	The requirement meets this objective by ensuring that the TOE collects information about allowed and disallowed changes to objects and execution of programs on the managed systems.
O.ANALYZE The TOE must apply analytical processes and information to derive conclusions about allowed and disallowed accesses to objects.	EXT_MAC_ANL.1 Application and change control analysis	The requirement meets this objective by ensuring that the TOE analyzes the collected change control and application control events and actions.
O.REACT The TOE shall take appropriate action on all allowed and disallowed accesses to objects.	EXT_MAC_RCT.1 Application and change control react	The requirement meets this objective by ensuring that the TOE takes appropriate actions, as defined by policy, on all allowed and disallowed accesses to objects.

8.5.2 Security Assurance Requirements Rationale

EAL3 was chosen to provide a moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL3, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 19 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 19 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	Although FPT_STM.1 is not included, the TOE Environment provides reliable timestamps to the TOE. An environmental objective states that the TOE will receive reliable timestamps, thereby satisfying this dependency.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.2	FAU_SAR.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FCS_COP.1	FCS_CKM.1	✓	This dependency is not met nor required for this Security Target because the user data protection is not the primary functionality of this TOE.
	FCS_CKM.4	✓	This dependency is not met nor required for this Security Target because the user data protection is not the primary functionality of this TOE.
FIA_ATD.1	No dependencies		
FIA_UID.2	No dependencies		
FIA_USB.1	FIA_ATD.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies		

SFR ID	Dependencies	Dependency Met	Rationale
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FPT_ITT.1	No dependencies		
EXT_MAC_SDC.1	No dependencies		
EXT_MAC_ANL.1	EXT_MAC_SDC.1	✓	
EXT_MAC_RCT.1	EXT_MAC_ANL.1	✓	
	EXT_MAC_SDC.1	✓	

9 Acronyms

This section describes the acronyms.

9.1 Acronyms

Table 20 – Acronyms

Acronym	Definition
ACL	Access Control List
ADS	Alternate Data Stream
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CM	Configuration Management
DNS	Domain Name System
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MS	Microsoft
NFS	Network File Server
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
RSD	Rogue System Detection
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
UNC	Universal Naming Convention

Prepared by:
Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com