SECURITY TARGET

MCAFEE® HERCULES® POLICY AUDITOR AND MCAFEE® HERCULES® REMEDIATION MANAGER (MCAFEE® HERCULES®)

VERSION 4.5

Document No. 1566-001-D001

Version 1.3, 9 April 2008

Prepared for:

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

Prepared by:

Electronic Warfare Associates-Canada, Ltd.
55 Metcalfe St., Suite 1600
Ottawa, Ontario
K1P 6L5

Security Target

McAfee® Hercules® Policy Auditor and McAfee® Hercules® Remediation Manager (McAfee® Hercules®)

Version 4.5

Document No. 1566-001-D001

Version 1.3, 9 April 2008

<Original> Approved by:

Project Engineer:	Ben Cuthbert	09 April 2008
Project Manager:	Grant Gibbs	09 April 2008
Program Director:	Erin Connor	09 April 2008
	(Signature)	(Date)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 GENERAL

This introductory section presents security target (ST) identification information, an overview of the product and an overview of the ST structure. A brief discussion of the ST development methodology is also provided.

An ST document provides the basis for the evaluation of an information technology (IT) product or system under the Common Criteria for Information Technology Security Evaluation (CC). Within the ST the product or system which is being evaluated is referred to as the Target of Evaluation (TOE). An ST principally defines:

- A set of assumptions about the security aspects of the environment, a list of threats which the product is intended to counter, and any known rules with which the product must comply (see Section 3, Security Environment).
- A set of security objectives and a set of security requirements are presented in Sections 4 and 5, Security Objectives and IT Security Requirements, respectively.
- The IT security functions provided by the TOE which meet that set of requirements (see Section 6, TOE Summary Specification).

The structure and contents of this ST comply with the requirements specified in the CC, Part 1, Annex B and Part 3, Chapter 8.

1.2 IDENTIFICATION

Title:	Security Target McAfee® Hercules® Policy Auditor and McAfee® Hercules® Remediation Manager (McAfee® Hercules®) Version 4.5
Publication Date:	09 April 2008
TOE:	McAfee® Hercules® Policy Auditor and McAfee® Hercules® Remediation Manager
Registration:	383-4-88
Common Criteria Conformance Claim:	The TOE is CC Part 2 conformant and CC Part 3 conformant.
Evaluation Assurance Level (EAL):	The TOE is EAL 3 conformant.
Protection Profile Conformance:	The TOE does not claim conformance with any Protection Profile (PP).

Common Criteria Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005, with all current approved interpretations.
International Standard:	ISO/IEC 15408:2005
Authors:	This document has been written by EWA-Canada on behalf of McAfee, Inc.

1.3 PRODUCT OVERVIEW

The McAfee® Hercules® is a vulnerability remediation and risk and compliance tool.

The purpose of the product is to demonstrate compliance with a security policy and enforce compliance with automated remediation of noncompliant or vulnerable systems. These functions can be performed on a heterogeneous network consisting of Microsoft® Windows®, Solaris™, Red Hat® Linux®, HP-UX®, AIX®, Tru64®, and Mac OS® X clients. The McAfee® Hercules® server requires Microsoft® Windows® Server 2003 SP1.

McAfee® Hercules® provides network security administrators with the ability to prioritize and remediate vulnerabilities using automated fixes that have been developed, tested, verified as being correct and validated as being appropriate, by trusted and dedicated IT security professionals.

New vulnerabilities are being discovered on a daily basis. It has been estimated that it takes approximately one hour of labour to manually correct one vulnerability on one client machine. For all but the smallest networks, manually correcting vulnerabilities imposes an unacceptable workload and cost for valuable and often scarce network and security administration resources. The McAfee® Hercules® product overcomes this problem. McAfee® Hercules® offers the following significant features:

- Interoperability – McAfee® Hercules® supports many industry leading vulnerability assessment scanners. For the complete list see F.IMPDATA.
- Multi-tiered Architecture – The McAfee® Hercules® Administrator Console can be configured to manage multiple McAfee® Hercules® Servers.
- Administrator Control – Administrators maintain complete control over the selection of which vulnerabilities are to be remediated.
- Multiple O/S Support –McAfee® Hercules® supports Microsoft® Windows®, Solaris™, Red Hat® Linux®, HP-UX®, AIX®, Tru64®, and Mac OS® X.
- Reporting – Detailed reports organize the vulnerability remediation data and can be used to measure the ongoing success of frequent vulnerability remediation cycles. In

enterprise reporting mode, these reports may be aggregated to report data across multiple servers.

- Consistent Remediation – McAfee® Hercules® provides a consistent method of remediation across an entire network; it does not depend on the skill level of individual technicians when resolving vulnerabilities.

- Device Grouping – Administrators can place devices into logical groups and schedule remediation by groups.

- Device Discovery – Discovery of network devices from a Windows® Active Directory or NT Domain structure as well as importing from a flat file or user-defined IP address range.

- Device Inventory – With AssetGuard, users are able to perform inventory data collection on specific devices.

- Device Query – This search mechanism can use inventoried device data properties in their query when locating devices that match a specific criteria.

- ActionPacks – Administrators can associate groups of vulnerabilities with Device Queries, allowing for an accurate application of security policy enforcement.

- Enhanced Security – Inclusion of pre-defined roles for role-based authentication and device group access control. Pre-defined tasks for use with roles that correspond to major functions that can be performed by the McAfee® Hercules® Administrator.

- Roll-back Capabilities – Administrators have the ability to roll-back system changes and patch installations when necessary.

- V-Flash – Administrators can stay current on the latest vulnerability remediation signatures through the McAfee® Hercules® V-Flash update service.

- Remediation Policies – Users can define remediation policies for a single device or group of devices.

- Compliance-Only capability – Users assigned the policy auditor role can evaluate compliance of their network devices to policies without the ability to automate the remediation of vulnerabilities on non-compliant devices.

- Policy Enforcement – When you enforce a policy, remedies are applied regardless of detected vulnerabilities. With ConnectGuard™, disconnected machines are prevented from gaining access to the network until remedies have been applied that comply with the organizations security policy.

- Best Practices – McAfee® Hercules® offers complete support for the ‘best practices’ of vulnerability remediation.

- Optional Distributed Architecture – Remote deployment of the McAfee® Hercules® Channel Server and File Download Server components allow for an improved flow of data to areas that are geographically distant or across wide enterprise networks, thus optimizing network bandwidth and server capacity. (In a basic configuration the McAfee® Hercules® Server component encompasses the Channel Server and File Download Server on one platform).

At a high level, McAfee® Hercules® is designed to:

- Aggregate vulnerability and remediation information from leading sources including SecurityFocus, BugTraq, CERTs and other internet sources.
- Import scan information from vulnerability scanners and combine this information to perform remediation from a single source.
- Create profiles and remediation signatures that match scanner-independent vulnerability information and client machines with their corresponding remediations.
- Allow an administrator to target network machines for automated remediation.
- Support CVE compliance by displaying CVE identifiers and supporting searching using these identifiers.

Fundamentally, the McAfee® Hercules® product provides enterprise administrators with the ability to manage a large-scale vulnerability remediation process in a manner that is both systematic and comprehensive. Today many organizations employ an incomplete hybrid of manual and partially automated techniques that are often implemented in an ad-hoc manner. McAfee® Hercules® is a tool that is intended to bring a defined and systematic maturity into these security-critical processes.

In a Windows® environment, McAfee® Hercules® is a product that provides and includes all of the functionality typically associated with the vulnerability remediation capabilities of commercial and open source vulnerability scanners. These typically provide registry fixes for Windows® machines. However, this type of vulnerability only represents a small sub-set of the vulnerabilities that require remediation. The McAfee® Hercules® product expands this set to include the automated remediation of vulnerabilities associated with the following five classes of vulnerabilities:

- **Software Defects** – Hot fixes, patches, registry settings, etc.
- **Unnecessary/Insecure Services** – Telnet, Remote Access, FTP etc.
- **Insecure Accounts** – Null Passwords, Admin No Password, etc.
- **Back Doors** – NetBus, BackOrifice, SubSeven etc.
- **Miss-Configurations** – NetBIOS, file system privileges, Null Sessions etc.

The McAfee® Hercules® product is designed to operate on standard TCP/IP networks and can remediate vulnerabilities on Microsoft® Windows®, Solaris™, Red Hat® Linux®, HP-UX®, AIX®, Tru64®, and Mac OS® X based clients.

The McAfee® Hercules® human machine interface (HMI) provides the user with complete control over the functionality of the product. The HMI allows the user to specify:

- An automated frequency with which client systems will request updated vulnerability remediations.
- Manual remediations for selected client machines.
- Specific vulnerabilities which will not be remediated.

1.4 CONVENTIONS, TERMINOLOGY AND ACRONYMS

This section identifies the formatting conventions used to convey additional information and terminology having specific meaning. It also defines the meanings of abbreviations and acronyms used throughout the remainder of this document

1.4.1 Conventions

This section describes the conventions used to denote CC operations on security requirements and to distinguish text with special meaning. The notation, formatting and conventions used in this ST are largely consistent with those used in the CC. Selection presentation choices are discussed here to aid the ST reader.

The CC allows several operations to be performed on functional and assurance components; *assignment, iteration, refinement* and *selection* are defined in section 6.4.1.3.2 of the CC Part 1 v2.3.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment is indicated by showing the value in italicised text within square brackets [assignment: *values*].
- 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. There are no refinements within this ST.
- The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by italicised text within square brackets [selection: *value(s)*].
- The iteration operation is used to apply a security functional requirement to more than one aspect of the TOE. Iterations are denoted by assigning a number at the functional component level, e.g., “FDP_ACC.1, Subset access control (1)” and “FDP_ACC.1, Subset access control (2)”.

1.4.2 Terms

This section describes the terms that are used throughout this ST. When possible, terms are defined as they exist in the CC.

Assets	Information or resources to be protected by the countermeasures of a TOE.
Attack	An attempt to bypass security controls on an IT System. The attack may alter, release or deny data. Whether an attack will succeed depends on the vulnerability of the IT System and the effectiveness of existing countermeasures.
Audit	The independent examination of records and activities to ensure compliance with established controls, policy and operational procedures and to recommend indicated changes in controls, policy or procedures.
Audit Trail	In an IT System, a chronological record of system resource usage, this includes user login, file access or other activities and whether any actual or attempted security violations occurred, legitimate and unauthorised.
Authentication	To establish the validity of a claimed user or object.
Availability	Assuring information and communications services will be ready for use when expected.
Compromise	An intrusion into an IT System where unauthorised disclosure, modification or destruction of sensitive information may have occurred.
Confidentiality	Assuring information will be kept secret, with access limited to appropriate persons.
Evaluation	Assessment of a PP, a ST or a TOE, against defined criteria.
Information Technology (IT) System	May range from a computer system to a computer network.
Integrity	Assuring information will not be accidentally or maliciously altered or destroyed.
IT Product	A package of IT software, firmware and/or hardware providing functionality designed for use or incorporation

	within a multiplicity of systems.
Network	Two or more machines interconnected for communications.
Protection Profile (PP)	An implementation independent set of security requirements for a category of TOE that meet specific consumer needs.
Security	A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.
Security Policy	The set of laws, rules and practices that regulate how an organisation manages, protects and distributes sensitive information.
Security Target (ST)	A set of security requirements and specification to be used as the basis for evaluation of an identified TOE.
Target of Evaluation (TOE)	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
Threat	The means through which the ability or intent of a threat agent to adversely affect an automated system, facility or operation can be manifest. A potential violation of security.
TOE Security Functions (TSF)	A set of all hardware, software and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected and distributed within a TOE.
TSF Data	Data created by and for the TOE that might affect the operation of the TOE.
TSF Scope of Control	The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
User	An entity (human user or external IT entity) outside of the TOE that interacts with the TOE.
Vulnerability	Hardware, firmware or software flaw that leaves an IT System open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls and so forth that could be exploited by a threat to gain unauthorised access to information, unauthorised privileges or disrupt critical

processing.

1.4.3 Acronyms

CC	Common Criteria for Information Technology Security Evaluation
CERT	Computer Emergency Response Team
CM	Configuration Management
CVE	Common Vulnerabilities and Exposures
EAL	Evaluation Assurance Level
ePO	McAfee ePolicy Orchestrator
HMI	Human Machine Interface
IT	Information Technology
O/S	Operating System
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCP/IP	Transmission Control Protocol / Internet Protocol
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

2 TARGET OF EVALUATION DESCRIPTION

2.1 EVALUATED CONFIGURATIONS

2.1.1 Overview

The McAfee® Hercules® product is designed to facilitate the automatic vulnerability remediation of devices on a network. The product imports vulnerability information from a number of third party commercial vulnerability scanner products and consolidates this information into a single view of the vulnerabilities of each device in the network. The product provides a sequence of automatically executable remediation steps which will correct each recognized vulnerability. Users of the product may download new signatures from the 'V-Flash' server operated by McAfee®. The McAfee® Hercules® product provides an interface which allows users to view the listed vulnerabilities of devices on the network. Logical groupings of devices may be defined. An automatic remediation schedule may be defined for a group. In addition, a specific list of vulnerabilities to be remediated may be defined for the group.

The McAfee® Hercules® product is to be evaluated in two configurations:

- Standalone; and
- Distributed.

The two configurations are described in separate sections below. They contain the same components, and differ only in packaging. The TOE is software only and is identified as build 4.5.

2.1.2 Standalone

The Standalone configuration of the McAfee® Hercules® product is shown in Figure 1.

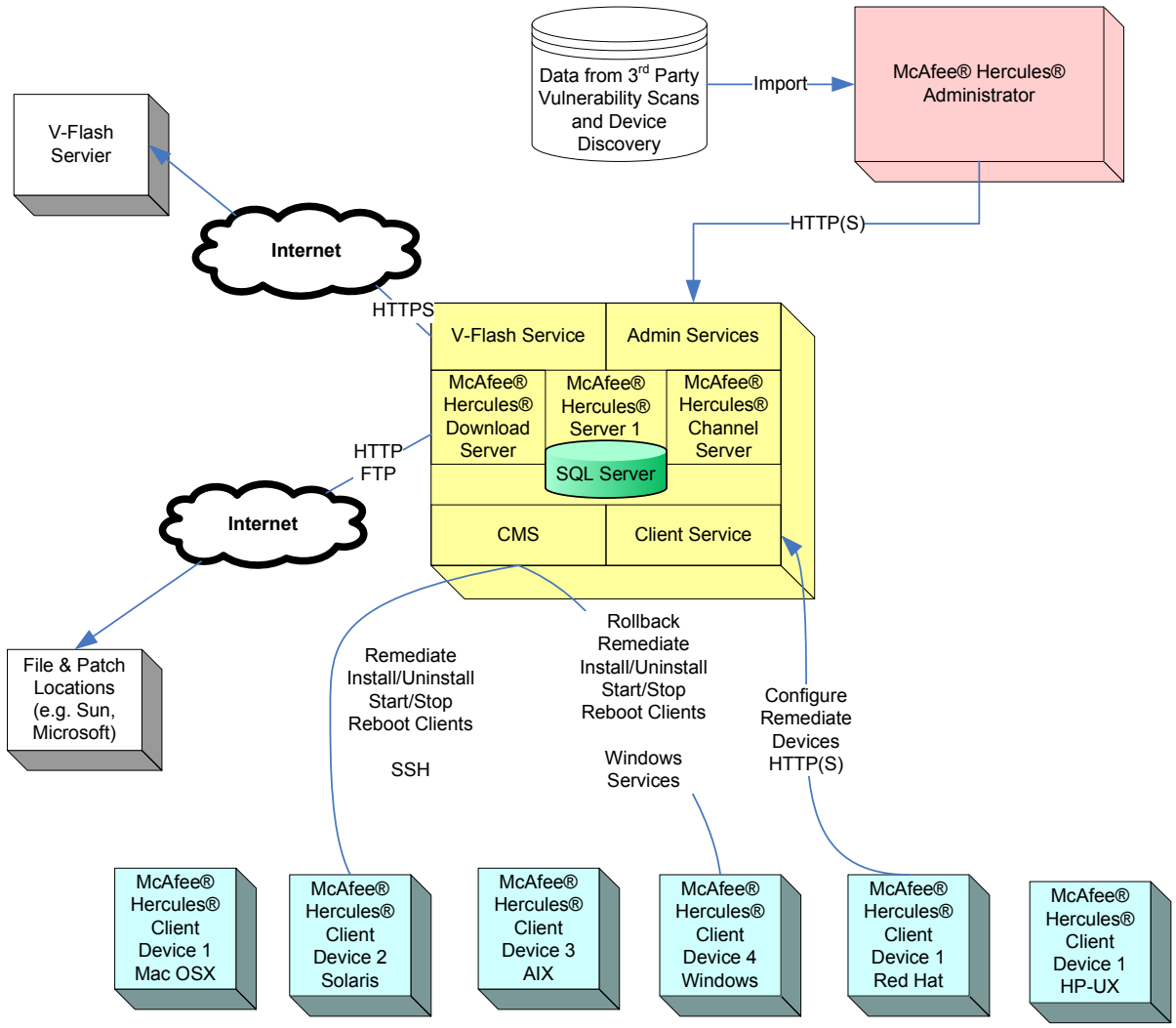

Figure 1 - McAfee® Hercules® Standalone Network Architecture

The McAfee® Hercules® Version 4.5 product consists of:

a. The McAfee® Hercules® Administrator Console executing on an Intel® Pentium compatible based PC running Windows® 2000 Server with Service Pack 4, Windows® 2000 Advanced Server with Service Pack 4, Windows 2000 Professional with Service Pack 4, Windows® XP Professional with Service Pack 2, Windows® Server 2003 Standard Edition with Service Pack 1, Windows® Server 2003 Enterprise Edition with Service Pack 1, Windows Vista Business or Windows Vista Enterprise as the operating system. Internet Explorer 5.5 or above, Microsoft .NET Framework v1.1 SP2, and Adobe Acrobat Reader™ 7.0 or higher are also required. If the McAfee® Hercules® Administrator Console is running on Windows® 2000, the Windows® 2000 High Encryption Pack is required. The minimum hardware requirements for the McAfee® Hercules® Administrator Console are specified in the

McAfee® Hercules® Installation Guide. The required setup of the McAfee® Hercules® Administrator Console is described in the McAfee® Hercules® Security Configuration Guide.

b. One or more McAfee® Hercules® Server(s) executing on an Intel® Pentium compatible based PC running Windows® Server 2003 Standard Edition with Service Pack 1 or Windows® Server 2003 Enterprise Edition with Service Pack 1 as the operating system. IIS 6.0 is also required. Internet Explorer 6.0 and Microsoft SQL Server 2005, Microsoft Reporting Services, Microsoft .NET Framework v1.1 SP2, Microsoft ASP.Net are required for all installations. The minimum hardware requirements for a McAfee® Hercules® Server are specified in the McAfee® Hercules® Installation Guide. The required setup of a McAfee® Hercules® Server is described in the McAfee® Hercules® Security Configuration Guide.

c. One or more network devices with McAfee® Hercules® Client Version 4.5 installed on a supported Windows® operating system. The supported versions of the Windows® operating system are Windows® NT 4.0 Workstation with Service Pack 6, Windows® NT 4.0 Standard Server with Service Pack 6, Windows® NT 4.0 Terminal Server with Service Pack 6, Windows® 2000 Professional, Windows® 2000 Server, Windows® 2000 Advanced Server, Windows® XP Professional, Windows® Server 2003 Standard Edition, Windows® Server 2003 Enterprise Edition, Windows® Vista Home Basic, Windows® Vista Home Premium, Windows® Vista Business, Windows® Vista Enterprise and Windows® Vista Ultimate. For Windows® NT 4.0 platforms, Internet Explorer 5.5 with Service Pack 2 or above is also required. The minimum system requirements for Windows® Clients are specified in the McAfee® Hercules® Enterprise Installation Guide.

d. One or more network devices with McAfee® Hercules® Client Version 4.5 installed on a supported version of the UNIX operating system. The supported versions of the UNIX operating system are Solaris™ 2.6, 7, 8, 9, 10; Red Hat® Desktop 7.3, 8, 9; Red Hat® Enterprise Linux (AS, EW, WS) 2.1, 3.0, 4.0; AIX® 5.1, 5.2, 5.3; HP-UX® 11.0, 11iv1; and Tru64® 5.1B. OpenSSH v3.5p1 or higher, SSL/HTTPS enabled with OpenSSL 0.96 or higher, sudo v1.6.7 or later are also required. The minimum system requirements for UNIX Clients are specified in the McAfee® Hercules® Installation Guide.

e. One or more network devices with McAfee® Hercules® Client Version 4.5 installed on a supported version of the Mac operating system. The supported versions of the Mac operating system are Mac OS X 10.2, 10.3, and 10.4. OpenSSH v3.5p1 or higher, SSL/HTTPS enabled with OpenSSL 0.96 or higher, sudo v1.6.7 or later are also required. The minimum system requirements for Mac Clients are specified in the McAfee® Hercules® Installation Guide.

2.1.3 Distributed

The distributed McAfee® Hercules® configuration is shown in Figure 2. In this configuration, the McAfee® Hercules® Channel Server and the McAfee® Hercules®

Download Server may be installed separately from the McAfee® Hercules® Server. The McAfee® Hercules® Channel Server and the McAfee® Hercules® Download Server have the same operating system support requirements as the McAfee® Hercules® Server.

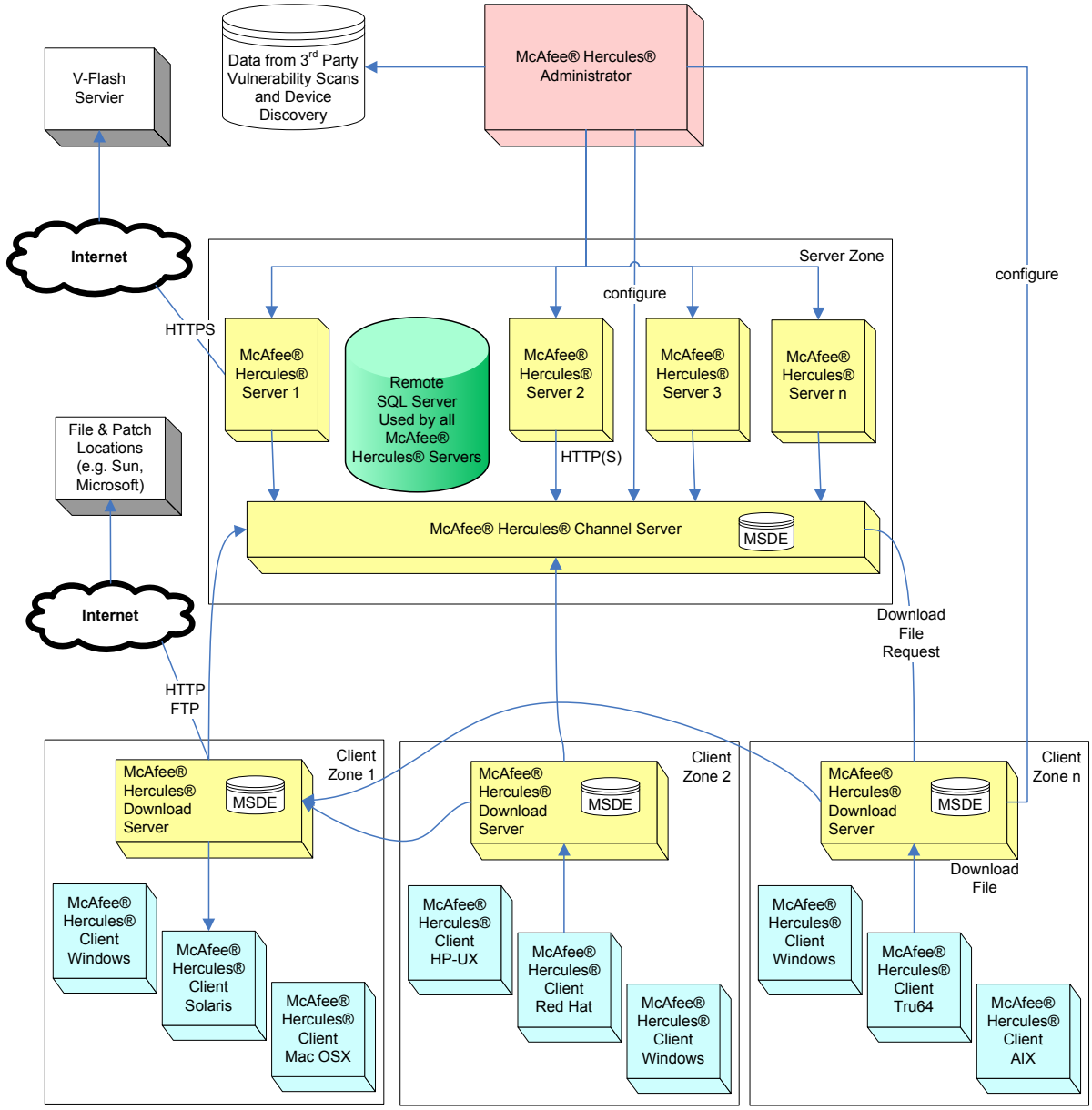

Figure 2 - McAfee® Hercules® Distributed Network Architecture

2.2 TOE BOUNDARY

2.2.1 Physical Boundary

The TOE Boundary for the McAfee® Hercules® product is shown in Figure 3. The TOE consists of:

a. the Administrator Console software;

b. the McAfee® Hercules® Server software;

c. the Channel Server software;

d. the Download Server software;

e. the UNIX Client software;

f. the Windows Client software; and

g. the Mac Client software.

The TOE operates in an environment that consists of:

a. the operating systems supporting the TOE software;

b. the hardware platforms on which the TOE software runs; and

c. third party software supporting the TOE software.

All interaction between the parts of the TOE takes place through the intermediary of the environment and the externals interact with the TOE through the intermediary of the environment.

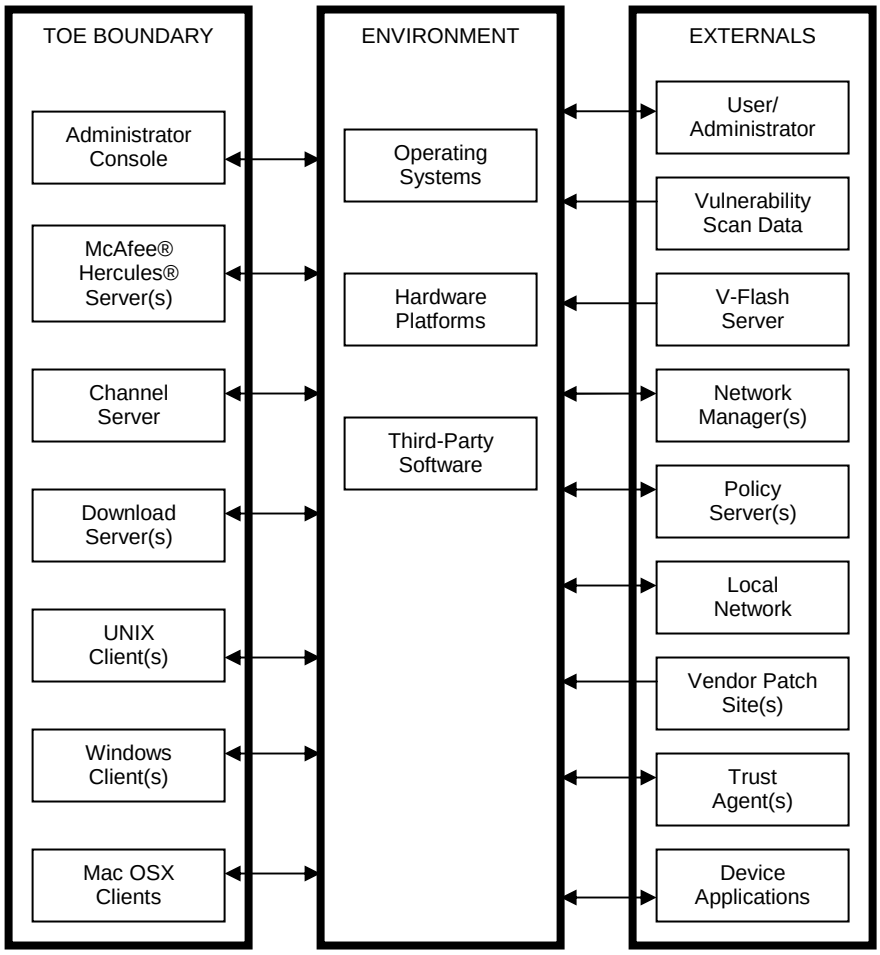

Figure 3 - TOE Boundary Diagram

The third-party software supporting the TOE consists of

a. Adobe Acrobat;

b. Microsoft SQL Server;

c. Microsoft Reporting Services;

d. InstallShield installer;

e. WodSSH library for SSH communications; and

f. Infragistics Windows Control Library.

These software products are obtained as compiled libraries and linked to the McAfee® code or as standalone applications that are interfaced to the McAfee® product.

2.2.2 Logical Boundary

The McAfee® Hercules® product is designed for the use of network administrators and it is assumed that these users are appropriately trained and experienced. Further, it is assumed that the user does not have malicious intent and configures the product and its host platforms in accordance with the guidance documentation. The product will not prevent a user from carelessly configuring or using the McAfee® Hercules® such that network protection is compromised.

Each major component of the McAfee® Hercules® product identified in the previous section contribute to the functionality provided by the TOE as a whole. This functionality is summarized by component below:

- The ***McAfee® Hercules® Administrator Console*** provides the HMI for the product. It uses SSL-based communications with the McAfee® Hercules® Server(s), and has the ability to interact with Windows® user accounts, domain privileges and NTFS privileges. It authenticates (using Windows® integrated authentication) to Internet Information Server on the McAfee® Hercules® server. The McAfee® Hercules® Administrator Console is designed to be installed and used on a trusted and appropriately configured and controlled Windows® machine that is used for network administration. Users of the McAfee® Hercules® Administrator Console require full administrative privileges on the machine running the console as well as the McAfee® Hercules® Server and all client machines. The McAfee® Hercules® Administrator Console provides the HMI for the product and includes the display and input devices through which the user interacts with the McAfee® Hercules® application. Information that can be gathered from this HMI include connected client systems, client status, list of vulnerabilities that will be remediated on a particular client or group of clients, remediation status, remediation signatures, scanner data, and vulnerabilities found on clients.

- The ***McAfee® Hercules® Server*** using a basic configuration comprising the McAfee® Hercules® Server, McAfee® Hercules® Download Server, and McAfee® Hercules® Channel Server Windows® service(s) that communicates with the McAfee® Hercules® Client to distribute remediation profiles and gather remediation progress data. Multiple McAfee® Hercules® Servers may be deployed within a network and administered from a single McAfee® Hercules® Administrator Console. The McAfee® Hercules® Server is designed to be installed and used on a trusted and appropriately configured and controlled Windows® server. This component also generates audit events in the log, including start, stop, successful actions and failed actions. The McAfee® Hercules® Server supports the export of user data for backup and transfer purposes as well as the import of remediation data, scanner data and device identifiers. Support for importing data in third party vulnerability scanner data is also supported. Remediation data, remediation profiles and roles can be managed through this component. Remediation profiles can be approved and then the profile data, along with remediation data, can be pushed out to client

systems. The Server receives remediation status back from the client. Remediation activities can be scheduled to be performed on a single client, or a group of clients.

- The ***McAfee® Hercules® Windows® Clients*** are services that perform remediation activities on client machines. The clients establish HTTPS/SSL-based communication to the McAfee® Hercules® Server. This component also generates audit events in the log, including start, stop, successful actions and failed actions. These audit events can be generated in the Windows® Event Viewer application's security and system categories. This component receives remediation and policy data that was pushed from the McAfee® Hercules® Server and then uses that data to remediate client systems and enforce the policy on the client. The remediation status is then reported back to the McAfee® Hercules® Server. Windows® Clients also support rollback of a remediation.

- The ***McAfee® Hercules® Unix Clients,*** provide functionality which is equivalent to Windows® client capabilities. Unix clients require a root account to install, configure, and execute Unix daemons, use of Unix file system access control and the use of ssh for installation. This component also generates audit events in the log, including start, stop, successful actions and failed actions. This component receives remediation and policy data that was pushed from the McAfee® Hercules® Server and then uses that data to remediate client systems and enforce the policy on the client. The remediation status is then reported back to the McAfee® Hercules® Server.

- The ***McAfee® Hercules® Mac Clients,*** provide functionality which is equivalent to Windows® client capabilities. Mac clients require a root account to install, configure, and execute Mac daemons, use of pseudo access control and the use of ssh for installation. This component also generates audit events in the log, including start, stop, successful actions and failed actions. This component receives remediation and policy data that was pushed from the McAfee® Hercules® Server and then uses that data to remediate client systems and enforce the policy on the client. The remediation status is then reported back to the McAfee® Hercules® Server.

3 TOE SECURITY ENVIRONMENT

3.1 ASSUMPTIONS

The following conditions are assumed to exist in the operational environment:

A.BACKUP	The organization operating the TOE has good backup and recovery procedures which are followed; allowing the TOE to be recovered to a secure configuration after a hardware failure.
A.CMS	In an environment where the McAfee® Hercules® client software is installed by remote means on a client machine using the McAfee® Hercules® Client Management Services (CMS), the server and clients are assumed to reside on a protected network.
A.CONFIG	The servers running the Remediation Manager and the Administrator Console have been configured securely as described in the Guidance documents and are maintained in that secure configuration. In particular: a. They are configured with the minimal operating system features installed and / or enabled to permit operation of the TOE. b. They are configured with minimal system privileges. c. They are configured with user accounts for authorized system administrators only and do not provide any end user accounts.
A.GOODOS	The Operating System of the client machines has been configured in accordance with the McAfee® Hercules® Security Configuration Guide and therefore may be trusted to function correctly for those OS functions required by the TOE component that is installed on the client machine.
A.KNOWLEDGE	TOE Users have knowledge of the operating systems on which the TOE resides, networking technology and general IT security practices.
A.NOEVIL	TOE Users are non hostile and follow all guidance documents.
A.PHYSICAL	The Server and Administrator elements of the TOE are physically secure and only authorized personnel have physical access to these elements of the TOE.
A.TOEUSER	Access to the TOE is restricted to authorized users. Authorized users are assigned to roles that in turn provide access to the administrative functions associated with that role. A TOE user is capable of performing only the administrative tasks inherited by their assigned roles. For the remainder of this document the phrase ‘TOE User’ shall be employed to represent any authorized user with administrative privileges.

3.2 THREATS

The threats discussed below are addressed by a compliant TOE. The threat agents are either human users or external IT entities not authorized to use the TOE. Additionally, threat agents may be users with administrative privileges that introduce vulnerabilities by inadvertently miss-configuring network systems from a security perspective. Threat agents are assumed to have a low level of sophistication, but may have knowledge of vulnerabilities and access to attack methods which are in the public domain. The TOE is not designed to withstand attack by sophisticated, highly motivated or well funded threat agents. The assets that are subject to attack are the components of the TOE itself and / or the resources of the client systems protected by the TOE.

T.BADDATA	A network attacker may attempt to provide the Remediation Manager with erroneous remediation information in an attempt to compromise the Client systems.
T.CLIENT	An unauthorized person may have administrator / root control of one of the client systems and may use that control to attempt to compromise the Remediation Manager.
T.CONSOLE	A network attacker may attempt to gain control of the TOE through the McAfee® Hercules® Administration Console.
T.EXPLOIT	A network attacker may attempt to exploit vulnerabilities on a client system protected by the TOE in order to gain unauthorized access to the resources of the client system.
T.NETEXPLOIT	A network attacker may attempt to exploit vulnerabilities on a client system protected by the TOE in an attempt to compromise other network resources.
T.OS	An unauthorized user may attempt to gain access over the operating system by bypassing a security mechanism and use this access to elevate his/her privileges over TOE functions and/or data.
T.REMSERVER	A network attacker may attempt to gain control of the McAfee® Hercules® Remediation Manager
T.SNIFF	A network attacker may intercept and monitor communications between the Remediation Manager and the Client systems and use the information gained to compromise the Remediation Manager and / or a Client system.
T.SNIFFSCAN	A network attacker may monitor communications between the Remediation Manager and a vulnerability scanner to learn vulnerabilities of client systems.
T.SPOOF	A network attacker may attempt to imitate the Remediation Manager and provide erroneous remediation information to a client system in order to compromise the client.

T.SPOOFCLIENT	A network attacker may attempt to imitate a client system in order to gain information about the vulnerabilities of the client system.
T.SPOOFSCAN	A network attacker may attempt to provide the Remediation Manager with erroneous vulnerability assessment information in an attempt to prevent the remediation of vulnerable network systems.

3.3 ORGANIZATIONAL SECURITY POLICIES

There is no requirement for the TOE to comply with any organizational security policy statements or rules.

4 SECURITY OBJECTIVES

4.1 SECURITY OBJECTIVES FOR THE TOE

O.ADMIN	The TOE must provide to authorized administrators a set of administrative functions that allow the effective management of TOE operations and security functions.
O.USERAUTH	The TOE must provide a mechanism for the identification and authentication of users to the TOE.
O.CLIENTPROT	The TOE must protect itself against attacks initiated by client systems.
O.CLIENTREM	The TOE must provide effective remediation of known and reported vulnerabilities for client systems.
O.HMI	The TOE must provide a controlled interface to its functionality such that only authorized TOE users are able to access the interface.
O.KNOWN	The TOE must ensure that legitimate users of the system are identified before rights of access can be granted.
O.NETATK	The TOE must protect itself against network attackers.
O.REMDATA	The TOE must ensure that its remediation data is obtained from trusted sources and must provide a mechanism to ensure the integrity of this data.
O.SCANDATA	The TOE must ensure that its scanner data is obtained from trusted sources and must provide a mechanism to ensure the confidentiality and integrity of this data.
O.USERDATA	The TOE must ensure that exported user data is secure.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

The list below details the security objectives for the environment in which the TOE resides. These objectives are to be met through the application of procedural and / or administrative measures. They do not impose any additional security requirements upon the TOE.

OE.AUTHUSER	Only authorized personnel are permitted physical access to the TOE.
OE.BACKUP	Good backup and recovery procedures for the TOE must be in place.
OE.DOMAIN	The host operating system will provide domain separation and ensure that the TOE cannot be tampered with.
OE.GOODOS	Those portions of the client operating system required for the correct operation of the TOE must function correctly.
OE.GOODUSER	Knowledgeable, non malicious users with system administrator privileges must be assigned to install, configure, administer, operate

	and maintain the TOE.
OE.GUIDANCE	The administrator(s) responsible for the TOE must ensure that the TOE is installed, configured, administered and operated in accordance with the guidance documents.
OE.PROTCOM	The operating system and environment in which the TOE is to be installed must support the use of digital certificates for identification and authentication as well as SSL/SSH protocols to support the protection of communications between components.
OE.SECURECOM	The network on which the TOE resides must protect the confidentiality and integrity of information exchanged between the distributed elements of the TOE when client machines are initially installed remotely using the McAfee® Hercules® Client Management Service (CMS).

5 IT SECURITY REQUIREMENTS

5.1 INTRODUCTION

Section 5 provides security functional and assurance requirements that must be satisfied by a compliant TOE operating in a defined environment. The requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC.

5.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for the TOE consist of the following components from Part 2 of the CC, summarized in Table 1.

CC Part 2 Security Functional Components	
Identifier	**Name**
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute based access control
FDP_ETC.1	Export of user data without security attributes
FDP_IFC.1 (1)	Subset information flow control
FDP_IFC.1 (2)	Subset information flow control
FDP_IFC.1 (3)	Subset information flow control
FDP_IFF.1 (1)	Simple security attributes
FDP_IFF.1 (2)	Simple security attributes
FDP_IFF.1 (3)	Simple security attributes
FDP_ITC.1	Import of user data without security attributes
FDP_ROL.1	Basic rollback
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UAU.6	Re-authenticating
FIA_UID.2	User identification before any action
FIA_USB.1	User-subject binding

CC Part 2 Security Functional Components	
Identifier	**Name**
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1 (1)	Management of security attributes
FMT_MSA.1 (2)	Management of security attributes
FMT_MSA.1 (3)	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data
FMT_REV.1	Revocation
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_RVM.1	Non-bypassability of the TSP

Table 1 - Summary of CC Part 2 Security Functional Requirements

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 [selection: *not specified*] level of audit; and
c) [assignment: *management of ActionPacks; management and control of McAfee® Hercules® Clients and the devices on which they are installed; device data import; device queries; device service; device group service; policy enforcement; policy service; remediation service; remedy group service; remedy service; role based security; server; V-Flash; vulnerability data import; and vulnerability service*].

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, 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 ST, [assignment: *no other audit relevant information*]

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.2	User identity association
Hierarchical to:	No other components.
FAU_GEN.2.1	The TSF shall be able to associate each auditable event with the identity of the user that caused the event.
Dependencies:	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification

FAU_SAR.1	Audit review

This component will provide authorised users the capability to obtain and interpret the information. In case of human users this information needs to be in a human understandable presentation. In case of external IT entities the information needs to be unambiguously represented in an electronic fashion.

Hierarchical to:	No other components.
FAU_SAR.1.1	The TSF shall provide [assignment: *all TOE user*s who are assigned to the Reporting Role] with the capability to read [assignment: *all McAfee® Hercules® logs*] 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

FDP_ACC.2	Complete access control
Hierarchical to:	FDP_ACC.1 Subset access control

FDP_ACC.2.1	The TSF shall enforce the [assignment: *ADMIN_ACCESS SFP*] on [assignment: *subjects: McAfee® Hercules® Administrator Console operating in response to authorized users, objects: McAfee® Hercules® Servers, McAfee® Hercules® Clients*] and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2	The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.
Dependencies:	FDP_ACF.1 Security attribute based access control

FDP_ACF.1	Security attribute based access control
Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [assignment: *ADMIN_ACCESS SFP*] to objects based on the following: [assignment: *subjects: McAfee® Hercules® Administrator Console operating in response to users;* *objects: McAfee® Hercules® Servers, McAfee® Hercules® Clients;* *security attributes: user identification, user assignment to role, role association with task*].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *user is assigned to a role that is authorized to perform the controlled operations on the controlled objects*].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *none*].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the [assignment: *user is not assigned to a role that is authorized to command the controlled subject (i.e., the default is to deny permission)*].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

FDP_ETC.1	Export of user data without security attributes
Hierarchical to:	No other components.
FDP_ETC.1.1	The TSF shall enforce the [assignment: EXCHANGE_SFP] when exporting user data, controlled under the SFP(s), outside of the TSC.
FDP_ETC.1.2	The TSF shall export the user data without the user data's associated security attributes.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_IFC.1	Subset information flow control (1)
Hierarchical to:	No other components.
FDP_IFC.1.1 (1)	The TSF shall enforce the [assignment: *IMPORT_SFP*] on [assignment: *McAfee® Hercules® Servers when importing vulnerability scan data and vulnerability remediation data from outside the TOE boundary*].
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.1	Subset information flow control (2)
Hierarchical to:	No other components.
FDP_IFC.1.1 (2)	The TSF shall enforce the [assignment: *EXCHANGE_SFP*] on [assignment: *McAfee® Hercules® Servers when exporting or importing vulnerability data, ActionPacks, custom policies, custom device queries, custom device query collections, and remedies via XML files across the TOE boundary*].
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.1	Subset information flow control (3)
Hierarchical to:	No other components.
FDP_IFC.1.1 (3)	The TSF shall enforce the [assignment: *CONNECT_SFP*] on [assignment: *McAfee® Hercules® Clients when determining the network traffic that is permitted to flow to and from the devices on which they reside*].
Dependencies:	FDP_IFF.1 Simple security attributes

FDP_IFF.1	Simple security attributes (1)
Hierarchical to:	No other components.
FDP_IFF.1.1 (1)	The TSF shall enforce the [assignment: *IMPORT_SFP*] based on the following types of subject and information security attributes: [assignment: *(1) The identification of an authorized TOE user; and (2) the format of the source data*].
FDP_IFF.1.2 (1)	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *(1) For the import of Vulnerability Scan data to the server; (a) the file to be imported has been specified by the authorized TOE User; and (2) The file meets the format expected by the TOE for the file purpose.*]
FDP_IFF.1.3 (1)	The TSF shall enforce the [assignment: *no additional information flow control SFP rule*s].
FDP_IFF.1.4 (1)	The TSF shall provide the following [assignment: *no additional SFP capabilitie*s].
FDP_IFF.1.5 (1)	The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *none*].
FDP_IFF.1.6 (1)	The TSF shall explicitly deny an information flow based on the following rules: [assignment: *none*].
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1	Simple security attributes (2)
Hierarchical to:	No other components.
FDP_IFF.1.1 (2)	The TSF shall enforce the [assignment: *EXCHANGE_SFP*] based on the following types of subject and information security attributes: [assignment: *(1) The identification and authentication of the TOE user; and (2) the format of the source data*].
FDP_IFF.1.2 (2)	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *(1)For the export of exchange data via XML files from the server, the data to be exported has been specified by the authorized TOE User; (2) For the import of exchange data via XML files to the server, (a) the file to be imported has been specified by the*

	authorized TOE User; and (b) the file meets the format expected by the TOE for the file purpose.]
FDP_IFF.1.3 (2)	The TSF shall enforce the [assignment: *no additional information flow control SFP rule*s].
FDP_IFF.1.4 (2)	The TSF shall provide the following [assignment: *no additional SFP capabilitie*s].
FDP_IFF.1.5 (2)	The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *none*].
FDP_IFF.1.6 (2)	The TSF shall explicitly deny an information flow based on the following rules: [assignment: *none*].
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1	Simple security attributes (3)
Hierarchical to:	No other components.
FDP_IFF.1.1 (3)	The TSF shall enforce the [assignment: *CONNECT_SFP*] based on the following types of subject and information security attributes: [assignment: *(1) The identification of the external device; (2) the remediation status of the external device; and (3) the defined Network Access Policy for network connection for the external device*].
FDP_IFF.1.2 (3)	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *For network access connection of remote devices, the remediation status of the external device satisfies the defined Network Access Policy for that device.*]
FDP_IFF.1.3 (3)	The TSF shall enforce the [assignment: *no additional information flow control SFP rule*s].
FDP_IFF.1.4 (3)	The TSF shall provide the following [assignment: *no additional SFP capabilitie*s].
FDP_IFF.1.5 (3)	The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *none*].
FDP_IFF.1.6 (3)	The TSF shall explicitly deny an information flow based on the following rules: [assignment: *none*].
Dependencies:	FDP_IFC.1 Subset information flow control

	FMT_MSA.3 Static attribute initialisation
FDP_ITC.1	Import of user data without security attributes
Hierarchical to:	No other components.
FDP_ITC.1.1	The TSF shall enforce the [assignment: *IMPORT_SFP, EXCHANGE_SFP*] when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: *no additional importation control rule*s].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation
FDP_ROL.1	Basic rollback
Hierarchical to:	No other components.
FDP_ROL.1.1	The TSF shall enforce [assignment: *SERVER_SFP*] to permit the rollback of the [assignment: *automatic vulnerability remediations*] on the [assignment: *Windows® client machines*].
FDP_ROL.1.2	The TSF shall permit operations to be rolled back within the [assignment: *time period between the completion of the remediation that is to be rolled back and the start of the next remediation*].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
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: [assignment: *user identification, user assignment to role*].
Dependencies:	No dependencies.

FIA_UAU.2	User authentication before any action
Hierarchical to:	FIA_UAU.1 Timing of authentication
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification

FIA_UAU.6	Re-authenticating
Hierarchical to:	No other components.
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions [assignment: *the user attempts to manage the McAfee® Hercules® Channel Server or the McAfee® Hercules® Download Server*].
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 identify itself 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: [assignment: *user identification*].

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: [assignment: *the TSF shall send the user identification with each request sent by a subject*].
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: [assignment: *none*].
Dependencies:	FIA_ATD.1 User attribute definition

FMT_MOF.1	Management of security functions behaviour
Hierarchical to:	No other components.
FMT_MOF.1.1	The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *administrative functions*] to [assignment: *the roles authorized by the ADMIN_ACCESS SFP*].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MSA.1	Management of security attributes (1)
Hierarchical to:	No other components.
FMT_MSA.1.1 (1)	The TSF shall enforce the [assignment: *SERVER_SFP*] to restrict the ability to [selection: *query*, [assignment: *none*]] the security attributes [assignment: *identification and authentication of client machine*] to [assignment: *McAfee® Hercules® Users authorized by the ADMIN_ACCESS SFP*].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions

FMT_MSA.1	Management of security attributes (2)
Hierarchical to:	No other components.
FMT_MSA.1.1 (2)	The TSF shall enforce the [assignment: *IMPORT_SFP*] to restrict the ability to [selection: *query*, [assignment: *none*]] the security attributes [assignment: *identification and authentication of client machine*] to [assignment: *McAfee® Hercules® Users authorized by the ADMIN_ACCESS SFP*].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions

FMT_MSA.1	Management of security attributes (3)
Hierarchical to:	No other components.
FMT_MSA.1.1 (3)	The TSF shall enforce the [assignment: *ADMIN_ACCESS SFP*] to restrict the ability to [selection: *create, modify, delete,* [assignment: *none*]] the security attributes [assignment: *user identification, assignment of users to roles*] to [assignment: *McAfee® Hercules® System Administrator*].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions

FMT_MSA.3	Static attribute initialisation
Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the [assignment: *IMPORT_SFP*] to provide [selection: *permissive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2	The TSF shall allow the [assignment: *authorised TOE users*] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MTD.1	Management of TSF data
Hierarchical to:	No other components.
FMT_MTD.1.1	The TSF shall restrict the ability to [selection: *modify, delete,* [assignment: *aggregate, display*]] the [assignment: *vulnerability data, remediation data and client system vulnerability and remediation status*] to [assignment: *McAfee® Hercules® users authorized by the ADMIN_ACCESS SFP*].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions
FMT_REV.1	Revocation
Hierarchical to:	No other components.
FMT_REV.1.1	The TSF shall restrict the ability to revoke security attributes associated with the [selection: *users, subjects, objects*, [assignment: *none*]] within the TSC to [assignment: *the roles authorized by the ADMIN_ACCESS SFP*].
FMT_REV.1.2	The TSF shall enforce the rules [assignment: *none*].
Dependencies:	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 security management functions: [assignment: *a. specifying a list of client systems which are to be subject to*

automatic vulnerability remediation;
b. specifying which vulnerabilities are to be remediated;
c. scheduling automatic vulnerability remediations;
d. rolling back previously completed remediations;
e. performing collection inventory;
f. managing compliance;
g. configuring network access; and
h. defining control policies].

Dependencies:	No dependencies

FMT_SMR.1	Security roles
Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [assignment: *as defined by the ADMIN_ACCESS SFP*].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification

FPT_RVM.1	Non-bypassability of the TSP
Hierarchical to:	No other components.
FPT_RVM.1.1	The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
Dependencies:	No dependencies.

5.3 SECURITY FUNCTIONAL REQUIREMENTS FOR THE IT ENVIRONMENT

The McAfee® Hercules® product relies upon the IT environment, which comprises the underlying operating system and third-party software, to provide some of the security features of the product. The security functional requirements for the IT environment consist of the following components from Part 2 of the CC, summarized in Table 2.

CC Part 2 Security Functional Components	
Identifier	**Name**
FAU_GEN.1€	Audit data generation
FAU_SAR.1€	Audit review
FAU_SEL.1€	Selective audit
FDP_IFC.1€	Information flow control
FDP_IFF.1€	Simple security attributes
FDP_ITT.1€	Basic internal transfer protection
FPT_ITT.1€	Basic internal TSF data transfer protection
FPT_RVM.1€	Non-bypassability of the TSP
FPT_SEP.1€	TSF Domain Separation
FPT_STM.1€	Reliable time stamps

Table 2 - Summary of Security Requirements for the Environment

€ – Denotes the environment iteration for this component

FAU_GEN.1€ Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1 The Environment 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 [selection: *not specified*] level of audit; and
c) [assignment: *use of the McAfee® Hercules® Client, McAfee® Hercules® Client Management Service, Patch Download Service or V-Flash Service events in addition to the audit capabilities of the underlying operating system*].

FAU_GEN.1.2 The Environment 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 ST, [assignment: *no other audit relevant information*]

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1€	Audit review

This component will provide authorised users the capability to obtain and interpret the information. In case of human users this information needs to be in a human understandable presentation. In case of external IT entities the information needs to be unambiguously represented in an electronic fashion.

Hierarchical to:	No other components.
FAU_SAR.1.1	The Environment shall provide [assignment: *authorised users*] with the capability to read [assignment: *log data retained by the Environment*] from the audit records.
FAU_SAR.1.2	The Environment shall provide the audit records in a manner suitable for the user to interpret the information.
Dependencies:	FAU_GEN.1 Audit data generation

FAU_SEL.1€	Selective audit
Hierarchical to:	No other components.
FAU_SEL.1.1	The Environment shall be able to include or exclude auditable events from the set of audited events based on the following attributes: a) [selection: *event type*] b) [assignment: *client machine identification*].
Dependencies:	FAU_GEN.1 Audit data generation FMT_MTD.1 Management of TSF data

FDP_IFC.1€	Subset information flow control
Hierarchical to:	No other components.
FDP_IFC.1.1	The Environment shall enforce the [assignment: *SERVER_SFP*] on [assignment: *McAfee® Hercules® Servers and client machines when the client machine requests a remediation profile from a McAfee® Hercules® Server*].
Dependencies:	FDP_IFF.1 Simple security attributes

FDP_IFF.1ϵ	Simple security attributes
Hierarchical to:	No other components.
FDP_IFF.1.1	The Environment shall enforce the [assignment: *SERVER_SFP*] based on the following types of subject and information security attributes: [assignment: *(1) Identification and authentication of the client machine; and (2) format of client machine remediation status information*].
FDP_IFF.1.2	The Environment shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *For the transfer of a remediation signature from the McAfee® Hercules® Server to a client machine; (a) the requesting client machine has been identified as authorised by the server using either certificates or in the absence of certificates the IP Address, Domain Name or NETBIOS name; and (b) the format of the client machine remediation status information is recognized.*
FDP_IFF.1.3	The Environment shall enforce the [assignment: *no additional information flow control SFP rule*s].
FDP_IFF.1.4	The Environment shall provide the following [assignment: *no additional SFP capabilitie*s].
FDP_IFF.1.5	The Environment shall explicitly authorise an information flow based on the following rules: [assignment: *none*].
FDP_IFF.1.6	The Environment shall explicitly deny an information flow based on the following rules: [assignment: *none*].
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation

FDP_ITT.1ϵ	Basic internal transfer protection
Hierarchical to:	No other components.
FDP_ITT.1.1	The Environment shall enforce the [assignment: *SERVER_SFP*] to prevent the [selection: *disclosure, modification*] of user data when it is transmitted between physically-separated parts of the TOE.

Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FPT_ITT.1€	Basic internal TSF data transfer protection
Hierarchical to:	No other components.
FPT_ITT.1.1	The Environment shall protect TSF data from [selection: *disclosure, modification*] when it is transmitted between separate parts of the TOE.
Dependencies:	No dependencies.
FPT_RVM.1€	Non-bypassability of the TSP
Hierarchical to:	No other components.
FPT_RVM.1.1	The Environment shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
Dependencies:	No dependencies.
FPT_SEP.1€	TSF domain separation
Hierarchical to:	No other components.
FPT_SEP.1.1	The Environment shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2	The Environment shall enforce separation between the security domains of subjects in the TSC.
Dependencies:	No dependencies.
FPT_STM.1€	Reliable time stamps
Hierarchical to:	No other components.

FPT_STM.1.1	The Environment shall be able to provide reliable time stamps to the TOE and for its own use.
Dependencies:	No dependencies.

5.4 INFORMATION FLOW CONTROL SECURITY FUNCTIONAL POLICIES

5.4.1 McAfee® Hercules® Server to Client Information Flow Control Security Functional Policy (SERVER_SFP)

The operating environment for the TOE consists of a McAfee® Hercules® Administrator Console and one or more McAfee® Hercules® Servers connected in a network with a number of client machines. It is expected that the client machines will contain vulnerabilities which will be automatically remediated by the McAfee® Hercules® Server on a scheduled basis. In an environment where the client machines are assumed to contain vulnerabilities the possibility always exists that one or more of the client machines have been compromised and may act maliciously towards the TOE. For this reason the only information that a McAfee® Hercules® Server will accept from any client machine is: (a) the identification of the client machine for authentication purposes when requesting a scheduled remediation, and (b) remediation status information during the course of a remediation session. All other information flow between the McAfee® Hercules® Server and a McAfee® Hercules® Client will consist of remediation profiles or rollback instructions (*Windows® client machines only)*, sent from the Server to the client.

5.4.2 Vulnerability Scanner Import Information Flow Control Security Functional Policy (IMPORT_SFP)

The TOE relies upon data generated by one or more third party vulnerability scanner products in order to identify the vulnerabilities which exist on client machines. These scanner products fall outside the boundary of the TOE. The data generated by the scanners is also initially outside the TOE boundary. However, authorised TOE users may import data from one of the recognised scanner products across the TOE boundary. If the vulnerability data is selected by an authorised TOE user and conforms to the expected format of data from one of the supported third party scanner products, then the TOE accepts that data as valid vulnerability information.

During the operation of the TOE the update of vulnerability remediation data must be performed on a regular basis. These updates are obtained from the trusted McAfee® Hercules® V-Flash server which falls outside the TOE boundary. The TOE uses SSL to ensure the fidelity of the data downloaded from the V-Flash server.

5.4.3 Data Exchange Information Flow Control Security Functional Policy (EXCHANGE_SFP)

The TOE allows authorised TOE users to export user data from a McAfee® Hercules® Server and import the exported data files to the same McAfee® Hercules® Server or to another McAfee® Hercules® Server. The export and subsequent import are controlled by the authorized user, who acts through the McAfee® Hercules® Administrator Console, which then controls the McAfee® Hercules® Server. This capability provides the ability to backup custom user data and an efficient means of transferring this data to a different McAfee® Hercules® Server.

The following data items may be transferred individually:

a. Vulnerabilities;

b. ActionPacks;

c. Custom Policies;

d. Custom Device Queries;

e. Custom Device Query Collections; and

f. Remedies.

The data is exported as XML files from the McAfee® Hercules® Server within the TOE Boundary to the Environment. The XML files in the TOE Environment are available for transfer to removable media or for transfer via the network.

Authorized TOE users may import the XML data files from the Environment to the McAfee® Hercules® Server across the TOE Boundary. If the XML file is selected by an authorised TOE user and conforms to the expected format of data, then the TOE accepts that data as valid information.

5.4.4 Administrator Access Control Security Functional Policy (ADMIN_ACCESS SFP)

The McAfee® Hercules® system incorporates a role-based access control capability that defines the tasks that authorized users are allowed to perform.

The McAfee® Hercules® system includes the following pre-defined roles:

a. McAfee® Hercules® System Administrator (SysA);

b. McAfee® Hercules® Server Administrator (SrvA);

c. McAfee® Hercules® Device Group Administrator (DGA);

d. McAfee® Hercules® Device Group User (DGU);

e. McAfee® Hercules® Remedy Writer (RemW);

f. McAfee® Hercules® Remediator (Rem);

g. McAfee® Hercules® Policy Auditor (CChk);

h. McAfee® Hercules® Importer (Imp); and

i. McAfee® Hercules® Reporter (Rep).

The McAfee® Hercules® system also enables the McAfee® Hercules® System Administrator to define new roles starting with no tasks assigned or starting from an existing role.

Each of the McAfee® Hercules® administrative tasks is associated with one or more roles. An authorized user must be assigned to a role that is associated with a task before the user can perform the task. A user may be assigned to more than one role, in which case the user is able to perform any task associated with any of the roles to which the user is assigned. A user that is not assigned to a role cannot perform any tasks.

5.4.5 Network Access Information Flow Control Security Functional Policy (CONNECT_SFP)

The TOE allows authorized TOE users to restrict the ability of external devices equipped with McAfee® Hercules® Clients to communicate over networks until they have been remediated. This connection restriction is controlled by the authorized user, who acts through the McAfee® Hercules® Administrator Console to direct the McAfee® Hercules® Client to limit the ability of the remote device to communicate over the network.

The following device access features are provided:

a. McAfee® Hercules® ConnectGuard blocks network traffic from remote and local client devices reconnecting to the network, checks devices for compliance with their assigned Network Access Policies (NAP), and applies the appropriate NAPs along with their remedy actions to noncompliant machines;

b. Cisco Systems Network Admission Control provides network access only to client devices that fully comply with the established NAP and ensures that noncompliant devices are denied access, placed into quarantine for remediation, or given restricted access to resources;

c. McAfee® Hercules® Network Access Policy is a corporate security policy that can be configured to ensure that an active antivirus is installed and running on client devices or to ensure protection from a specified set of vulnerabilities. The McAfee® Hercules® system provides a mechanism to apply the NAP and all remediations

associated with the policy to client devices to ensure that the devices are in compliance before they are allowed full access to the network.

5.5 TOE SECURITY ASSURANCE REQUIREMENTS

The security assurance requirements for the TOE comprise the requirements corresponding to the EAL 3 level of assurance as defined in the CC Part 3. The assurance components are summarized in the following table:

Assurance Class	**Assurance Components**	
	Identifier	**Name**
Configuration Management	ACM_CAP.3	Authorisation controls
	ACM_SCP.1	TOE CM coverage
Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Security enforcing high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle Support	ALC_DVS.1	Identification of security measures
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 3 - EAL 3 Assurance Requirements

6 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

A typical attacker in the intended environment for the TOE is assumed to have a low level of sophistication, but may have knowledge of vulnerabilities and access to attack methods that are in the public domain. The purpose of the attacks could be (1) to gain access to the resources of the TOE, (2) to gain access to the resources of the client systems protected by the TOE, and/or (3) to prevent the successful remediation of client systems and thus leave these systems in a vulnerable state. Therefore, the attack potential which is applicable for AVA_SOF.1 calculations is LOW. Any residual vulnerabilities may only be exploited by an attacker of moderate or high attack potential. The strength of function claim is therefore SOF-BASIC.

This claim applies to the security function F.IAUSER.

6.1 TOE SECURITY FUNCTIONS

A description of each of the TOE security functions follows.

F.ACCESS	Access Control Access to the TOE is restricted to authorized administrators through the use of user identification and authentication. The TOE has the capability of incorporating role-based access control. Each of the McAfee® Hercules® administrative tasks can be associated with one or more roles. An authorized user must be assigned to a role that is associated with a task before the user can perform the task.
F.AGGVADATA	Aggregate Scanner Data The TOE has the capability of merging vulnerability scanner information from the third party vulnerability scanners for a client machine into a single consistent vulnerability assessment for that machine.
F.APPPROF	Approve Profile The TOE provides the capability for a suitably authorized user to approve a remediation profile. Once approved the remediation profile shall be automatically invoked by each client machine in the group to which the profile applies at the next scheduled remediation interval.

F.AUDIT	Audit Remediation Activity The TOE maintains an audit trail of the remediation activities performed by each McAfee® Hercules® server. The McAfee® Hercules® server components and client systems create events in the logs which include stop, start, successful actions and failed actions. These events are created on the McAfee® Hercules® server and the target machine that is being remediated. The identity of the user who caused the event is also created on the McAfee® Hercules® server. For Windows® clients, the McAfee® Hercules® server is capable of generating audit events in the Windows® Event Viewer application's security and system categories.
F.DISPCLIENT	Display Network Client Systems The TOE has the capability of displaying, via a graphical user interface, a list of devices connected to a McAfee® Hercules® Server.
F.DISPCLIENTSTATUS	Display Network Client Status The TOE has the capability of displaying, via a graphical user interface, the operational status of each client machine.
F.DISPPROF	Display Profiles The TOE has the capability of displaying, via a graphical user interface, the list of vulnerabilities that will be remediated by the McAfee® Hercules® Server for a client machine or a group of client machines.
F.DISPREMSTATUS	Display Remediation Status The TOE has the capability of displaying. via a graphical user interface. the remediation status of each client machine of each McAfee® Hercules® Server.
F.DISPSIG	Display Remediation Signatures The TOE has the capability of displaying, via a graphical user interface, the steps required to remediate a specific vulnerability on a client machine.
F.DISPVADATA	Display Scanner Data The TOE has the capability of displaying imported scanner

	information.
F.DISPVULN	Display Vulnerabilities The TOE has the capability of displaying graphically the vulnerabilities on each machine on a network. It shall be possible to list all of the vulnerabilities reported for each and all machines on the network, or to display a list of machines which are susceptible to a specific vulnerability.
F.EXPORTDATA	Export Data Each McAfee® Hercules® Server has the capability to export user data for backup purposes or as an efficient means for transferring to another McAfee® Hercules® server.
F.IAUSER	Identify and Authenticate Users The McAfee® Hercules® Administrator Console has the capability to identify and authenticate users of the console both on initial start-up and when changing servers. The McAfee® Hercules® Administrator Console executes using a Windows® administrator account which is recognized by the machine hosting the McAfee® Hercules® server. Identification and authentication is achieved though the use of a username and password pair. This method of identification and authentication is also performed for the McAfee® Hercules® Channel Server and the McAfee® Hercules® Download Server.
F.IMPREMDATA	Import Remediation Data The TOE has the capability to import specific remediation information for reported vulnerabilities.
F.IMPDATA	Import Scanner Data The TOE has the capability of importing vulnerability scanner information from the following third party vulnerability scanners: 1. eEye® Digital Security Retina® Network Security Scanner 2. eEye Digital Security REM™ Security Management Console

3. Foundstone, Inc.® FoundScan Engine™
4. Harris STAT® Scanner
5. Harris STAT® Scanner 6.2.1 and above (Guardian)
6. Internet Security Systems™ Internet Scanner®
7. Internet Security Systems™ SiteProtector™
8. Internet Security Systems™ System Scanner™
9. Microsoft® Baseling Security Analyzer (MBSA)
10. nCircle® IP360™ Vulnerability Management System
11. NexantiS SecureScout SP™
12. Qualys™, Inc. QualysGuard® Scanner
13. Saint Corporation SAINT® Scanning Engine
14. Tenable Network Security™ Nessus Scanner
15. Tenable Network Security NeWT Scanner
16. The MITRE Corporation OVAL™ Definition Interpreter

F.IMPDEV Import Device Identifiers

The TOE can import device identifiers from the following:

1. Windows NT Domain
2. Windows Active Directory Domain
3. Flat File Import
4. User Definable IP address range
5. ePO asset information

F.MANAGEDATA	Manage Scanner and Remediation Data The TOE provides the user with an interface from which it is possible to manage the vulnerability scanner information and the vulnerability remediation information. A user may view a remediation profile for a device in order to determine which vulnerabilities and associated remedies will be applied to a device when it is remediated.
F.MANAGEPROF	Manage Profiles The TOE provides the capability for a suitably authorized user to manage remediation profiles. Machines may be added to or removed from the group to which the profile applies. Specific vulnerabilities may be added to or removed from the remediation profile.
F.MANAGEROLES	Manage Roles The TOE provides the capability for a suitably authorized user to create and manage custom roles for the TOE. Once created, individual users and groups of users may be assigned to the role. Privileges to use specific functions of the TOE such as creating custom remediation remedies, user defined vulnerabilities, and selectable pre-defined McAfee® Hercules® tasks may also be assigned to the role. The McAfee® Hercules® Server comes with predefined roles that restrict access to various tasks. Users assigned to these roles are not able to perform any other functions outside their role. A user may be a member of multiple roles. Restrictions to devices or device groups can be managed through the assignment of roles or available users to Device Groups.
F.PUSHREM	Push Remediation Data The McAfee® Hercules® Server provides remediation data in the form of a remediation profile to client machines.
F.PUSHPOLICY	Push Policy Data A client can be denied network access until remediation data has been pushed to the device that complies with the security of the organization. This can be accomplished through the use of McAfee® Hercules® ConnectGuard or Cisco Systems Network Admission Control (NAC), using a

	McAfee® Hercules® Network Access Policy (NAP).
F.REMCLIENT	Remediate Client System The TOE provides the capability to automatically remediate specific vulnerabilities on client machines.
F.REMPOLICY	Enforce Policy on Client Systems The TOE can enforce a remediation policy by enabling remedies that are part of a Remedy Group for a device or group of devices regardless of detected vulnerabilities for these device(s).
F.REPREMSTATUS	Report Remediation Status The TOE has the capability of producing reports describing the remediation status of each client machine of each McAfee® Hercules® Server. The user can select reports which show the details and summaries of: remediation sessions, import sessions, devices, groups, vulnerabilities, policies and remedies.
F.ROLLBACK	Rollback Remediation The TOE has the capability to systematically rollback the last remediation session performed on a Windows® client machine.
F.RVM	Reference Monitor The TOE provides reference mediation (e.g., when a user process requires access to a resource its requests a handle/token for the resource from the operating system). Reference mediation is supported by the operating system platform used by the TOE.
F.SCHEDREM	Schedule Remediation The TOE provides the capability to schedule remediation activities for a single client machine or groups of client machines.

6.2 ASSURANCE MEASURES

A description of each of the TOE assurance measures follows.

M.AUTH	The TOE includes documentation which describes the authorization controls used by the developer to ensure that only authorized modifications may be made to the TOE.
M.CONFIG	The TOE includes a configuration item list that identifies those items of the TOE that are subject to configuration control by the developer.
M.DELIVER	The TOE includes documentation describing the secure delivery of the TOE.
M.DESIGN	The TOE includes design documentation, which at a minimum consists of an informal functional specification, an informal high level design and an informal correspondence demonstration between the TOE Summary Specification, the Functional Specification and the High Level Design.
M.DEVELOP	The TOE includes documentation which describes the development security measures.
M.DOCS	The TOE includes user and administrator guidance documentation in the form of a User's Guide and an Installation Guide as well as an online help file, accessible from the TOE HMI.
M.ID	The TOE incorporates a unique version identifier that can be displayed to the user.
M.SETUP	The TOE includes an automated installation and set-up program compatible with the TOE operating system. The installation process includes sufficient instructions to clearly document the installation process. The default installation results in the secure installation and start-up of the TOE.
M.TEST	A suitably configured TOE has been evaluated in a controlled networked environment to confirm that TOE functionality operates as specified, and that the product can remediate a representative set of well-known vulnerabilities from each of the vulnerability classes claimed by the developer. TOE functionality has also been evaluated in a real-world environment, using a representative set of network systems configured with known vulnerabilities. The TOE includes developer test documentation which consists of test plans, test procedure descriptions, expected test results and actual test results. The test documentation is sufficient to determine that the developer has systematically tested the TOE against both the functional specification and the high level design.
M.VULNER	The TOE includes vulnerability documentation which describes the strength of function analysis along with an analysis of obvious vulnerabilities in the TOE.

7 PROTECTION PROFILE CLAIMS

This ST does not make compliance claims with respect to any Protection Profiles.

8 RATIONALE

8.1 SECURITY OBJECTIVES RATIONALE

Table 4 provides a bi-directional mapping of Security Objectives to Threats and Assumptions. It is followed by a discussion of how each Threat or Assumption is addressed by the corresponding Security Objective(s).

	O.ADMIN	O.USERAUTH	O.CLIENTPROT	O.CLIENTREM	O.HMI	O.KNOWN	O.NETATK	O.REMDATA	O.SCANDATA	O.USERDATA	OE.AUTHUSER	OE.BACKUP	OE.DOMAIN	OE.GOODOS	OE.GOODUSER	OE.GUIDANCE	OE.PROTCOM	OE.SECURECOM
A.BACKUP												X						
A.CMS																		X
A.CONFIG																X		
A.GOODOS														X				
A.KNOWLEDGE															X			
A.NOEVIL															X			
A.PHYSICAL											X							
A.TOEUSER															X			
T.BADDATA								X										
T.CLIENT			X															
T.CONSOLE	X	X			X	X	X			X								
T.EXPLOIT				X														
T.NETEXPLOIT				X														
T.OS													X					
T.REMSERVER							X											
T.SNIFF																	X	
T.SNIFFSCAN									X									
T.SPOOF																	X	
T.SPOOFCLIENT																	X	
T.SPOOFSCAN									X									

Table 4 - Mapping of Security Objectives to Threats and Assumptions

A.BACKUP	*The organization operating the TOE has good backup and recovery procedures which are followed; allowing the TOE to be recovered to a secure configuration after a hardware failure.* The OE.BACKUP objective details the need for good backup and recovery procedures.
A.CMS	*In an environment where the McAfee® Hercules® client software is installed by remote means on a client machine using the McAfee® Hercules® Client Management Services (CMS), the server and clients are assumed to reside on a protected network.* The OE.SECURECOM objective ensures that communications between the McAfee® Hercules® Server and client machines using CMS are protected.
A.CONFIG	*The servers running the Remediation Manager and the Administrator Console have been configured securely as described in the Guidance documents and are maintained in that secure configuration. In particular:* *a. They are configured with the minimal operating system features installed and / or enabled to permit operation of the TOE.* *b. They are configured with minimal system privileges.* *c. They are configured with user accounts for authorized system administrators only and do not provide any end user accounts.* The OE.GUIDANCE objective ensures that the TOE will be configured securely.
A.GOODOS	*The Operating System of the client machines has been configured in accordance with the McAfee® Hercules® Security Configuration Guide and therefore may be trusted to function correctly for those OS functions required by the TOE component that is installed on the client machine.* The OE.GOODOS objective ensures that those functions of the operating system required by the TOE function correctly.
A.KNOWLEDGE	*TOE Users have knowledge of the operating systems on which the TOE resides, networking technology and general IT security practices.* The OE.GOODUSER objective notes that TOE Users must be knowledgeable.
A.NOEVIL	*TOE Users are non hostile and follow all guidance documents.* The OE.GOODUSER objective notes that TOE Users must be non malicious.

A.PHYSICAL	*The Server and Administrator elements of the TOE are physically secure and only authorized personnel have physical access to these elements of the TOE.*
	The OE.AUTHUSER objective notes that only authorized personnel are permitted physical access to the TOE.
A.TOEUSER	*Access to the TOE is restricted to authorized users. Authorized users are assigned to roles that in turn provide access to the administrative functions associated with that role. A TOE user is capable of performing only the administrative tasks inherited by their assigned roles. For the remainder of this document the phrase 'TOE User' shall be employed to represent any authorized user with administrative privileges.*
	The OE.GOODUSER objective describes the characteristics of the TOE Users and notes that these users must be authorized system administrators.
T.BADDATA	*A network attacker may attempt to provide the Remediation Manager with erroneous remediation information in an attempt to compromise the Client systems.*
	The O.REMDATA objective ensures that the remediation data used by the TOE is accurate and secure.
T.CLIENT	*An unauthorized person may have administrator / root control of one of the client systems and may use that control to attempt to compromise the Remediation Manager.*
	The O.CLIENTPROT objective ensures that the TOE is protected against attacks by the client systems.
T.CONSOLE	*A network attacker may attempt to gain control of the TOE through the McAfee® Hercules® Administration Console.*
	The O.HMI, O.NETATK, and O.KNOWN objectives ensure that the Administration Console is secure. O.USERAUTH ensures the user has authenticated to the console and O.ADMIN ensures effective management of the TOE security functions provided to that user. O.USERDATA ensures exported user data is provided only to authorised users of the administration console.
T.EXPLOIT	*A network attacker may attempt to exploit vulnerabilities on a Client system protected by the TOE in order to gain unauthorized access to the resources of the client system.*
	The O.CLIENTREM objective ensures that the TOE provides effective remediation to client systems in order to remove or mitigate identified vulnerabilities.

T.NETEXPLOIT	*A network attacker may attempt to exploit vulnerabilities on a Client system protected by the TOE in an attempt to compromise other network resources.*
	The O.CLIENTREM objective ensures that the TOE provides effective remediation to client systems in order to remove or mitigate identified vulnerabilities.
T.OS	*An unauthorized user may attempt to gain access over the operating system by bypassing a security mechanism and use this access to elevate his/her privileges over TOE functions and/or data.*
	The OE.DOMAIN environment objective ensures that the host operating system on which the TOE resides provides domain separation.
T.REMSERVER	*A network attacker may attempt to gain control of the McAfee® Hercules® Remediation Manager*
	The O.NETATK objective ensures that the Remediation Manager is secure.
T.SNIFF	*A network attacker may monitor communications between the Remediation Manager and the Client systems and use the information gained to compromise the Remediation Manager and / or a Client system.*
	The OE.PROTCOM objective ensures that the information passing between the distributed parts of the TOE is secure.
T.SNIFFSCAN	*A network attacker may monitor communications between the Remediation Manager and a vulnerability scanner to learn vulnerabilities of client systems.*
	The O.SCANDATA objective ensures that the scanner data used by the TOE is accurate and secure.
T.SPOOF	*A network attacker may attempt to imitate the Remediation Manager and provide erroneous remediation information to a client system in order to compromise the client.*
	The OE.PROTCOM environment objective ensures that it is not possible to imitate the Remediation Manger.
T.SPOOFCLIENT	*A network attacker may attempt to imitate a client system in order to gain information about the vulnerabilities of the client system.*
	The OE.PROTCOM environment objective ensures that it is not possible for an attacker to imitate a client system.
T.SPOOFSCAN	*A network attacker may attempt to provide the Remediation Manager with erroneous vulnerability assessment information in an attempt to prevent the remediation of vulnerable network systems.*

The O.SCANDATA objective ensures that the scanner data used by the TOE is accurate and secure

8.2 SECURITY REQUIREMENTS RATIONALE

Table 5 provides a bi-directional mapping of Security Functional Requirements to Security Objectives, and is followed by a discussion of how each Security Objective is addressed by the corresponding Security Functional Requirements.

	O.ADMIN	O.USERAUTH	O.CLIENTPROT	O.CLIENTREM	O.HMI	O.KNOWN	O.NETATK	O.REMDATA	O.SCANDATA	O.USERDATA	OE.AUTHUSER	OE.BACKUP	OE.DOMAIN	OE.GOODOS	OE.GOODUSER	OE. GUIDANCE	OE.PROTCOM	OE.SEURECOM
FAU_ GEN.1			X	X	X		X	X	X									
FAU_GEN.2			X	X	X		X	X	X									
FAU_ SAR.1					X													
FAU_SAR.2					X													
FDP_ACC.2	X		X															
FDP_ACF.1	X		X															
FDP_ETC.1										X								
FDP_ IFC.1 (1)				X				X										
FDP_ IFC.1 (2)										X								
FDP_ IFC.1 (3)			X															
FDP_ IFF.1 (1)				X				X										
FDP_ IFF.1 (2)										X								
FDP_ IFF.1 (3)			X															
FDP_ ITC.1								X	X									
FDP_ROL.1				X														
FIA_ATD.1		X				X												
FIA_UAU.2		X	X		X		X	X										
FIA_UAU.6		X																
FIA_UID.2		X	X		X	X	X	X										
FIA_USB.1						X												
FMT_MOF.1	X																	
FMT_MSA.1 (1)				X	X	X												
FMT_MSA.1 (2)				X	X	X												
FMT_MSA.1 (3)	X				X	X												
FMT_ MSA.3				X	X													
FMT_MTD.1	X								X									
FMT_REV.1	X																	
FMT_SMF.1				X	X													
FMT_SMR.1	X				X													
FPT_RVM.1				X														
FAU_GEN.1є														X				

	O.ADMIN	O.USERAUTH	O.CLIENTPROT	O.CLIENTREM	O.HMI	O.KNOWN	O.NETATK	O.REMDATA	O.SCANDATA	O.USERDATA	OE.AUTHUSER	OE.BACKUP	OE.DOMAIN	OE.GOODOS	OE.GOODUSER	OE. GUIDANCE	OE.PROTCOM	OE.SEURECOM
FAU_SAR.1є														X				
FAU_SEL.1є														X				
FDP_IFC.1є			X	X													X	
FDP_IFF.1є			X	X													X	
FDP_ ITT.1є																	X	
FPT_ITT.1є																		X
FPT_RVM.1є				X														
FPT_SEP.1є													X					
FPT_STM.1є														X				

Table 5 - Mapping of Security Functional Requirements to Security Objectives

O.ADMIN *The TOE must provide to authorized administrators a set of administrative functions that allow the effective management of TOE operations and security functions.*

The TOE enforces ADMIN_ACCESS SFP administrator access control security functional policy (FDP_ACC.2, FDP_ACF.1, FMT_MOF.1, FMT_MSA.1 (3), FMT_MTD.1, FMT_REV.1, FMT_SMR.1)

O.USERAUTH *The TOE must provide a mechanism for the identification and authentication of users to the TOE.*

Identification and authentication functional requirements (FIA_UAU.2, FIA_UAU.6, FIA_UID.2, FIA_ATD.1) ensure that the identification and authentication activities complete successfully before information is transferred.

O.CLIENTPROT *The TOE must protect itself against attacks initiated by client systems.*

The TOE will only respond to requests for remediations which are received from identified and authorized client machines (FDP_IFC.1є, FDP_IFF.1є, FIA_UAU.2, FIA_UID.2). The TOE also enforces the ADMIN_ACCESS SFP administrator access control security functional policy to define the tasks that authorized users are allowed to perform (FDP_ACC.2, FDP_ACF.1). The TOE also maintains an audit trail of remediation requests, which may help

	to identify an attack from a client machine (FAU_GEN.1, FAU_GEN.2). The TOE also enforces CONNECT_SFP information flow control security functional policy to restrict the ability of external devices acting as Client Systems from communicating over networks until they have been remediated (FDP_IFC.1 (3), FDP_IFF.1 (3)).
O.CLIENTREM	*The TOE must provide effective remediation of known and reported vulnerabilities for client systems.* The TOE obtains its vulnerability and remediation data from trusted external sources using the IMPORT_SFP information flow control security function policy to govern the data import process (FDP_IFC.1 (1), FDP_IFF.1 (1)). The TOE protects its data from unauthorized modifications or corruption internally (FMT_MSA.1 (1), (2), FMT_MSA.3, FPT_RVM.1, FPT_RVM.1€). The TOE enforces the SERVER_SFP information flow control security functional policy when providing specific remediation data to authorized client systems (FDP_IFC.1€, FDP_IFF.1€). The TOE permits authorized users to configure the list of client systems and vulnerabilities, which will be remediated (FMT_SMF.1). Under specific circumstances the TOE is capable of rolling back remediations (FDP_ROL.1). Finally, the TOE maintains a comprehensive audit trail of its actions (FAU_GEN.1, FAU_GEN.2).
O.HMI	*The TOE must provide a controlled interface to its functionality such that only authorized TOE users are able to access the interface.* The TOE HMI is provided by the McAfee® Hercules® Administrator Console. This component of the TOE is only accessible to authorized administrative users (FIA_UAU.2, FIA_UID.2, FMT_SMR.1). Authorized users of the McAfee® Hercules® Administrator may control all of the security functions of the TOE, including setting security attributes and importing vulnerability scan and remediation data (FMT_MSA.1 (1) – (3), FMT_MSA.3, FMT_SMF.1). Actions performed by authorized users are subject to auditing (FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2).
O.KNOWN	*The TOE must ensure that legitimate users of the system are identified before rights of access can be granted.* The TOE identifies user security attributes for individual users (FIA_ATD.1, FIA_UID.2, FIA_USB.1, FMT_MSA.1 (1) – (3)).
O.NETATK	*The TOE must protect itself against network attackers.* The TOE protects itself against network attackers through its identification and authentication functions (FIA_UAU.2, FIA_UID.2). The collection of audit data (FAU_GEN.1,

	FAU_GEN.2) ensures that attacks of this type will be detected.
O.REMDATA	*The TOE must ensure that its remediation data is obtained from trusted sources and must provide a mechanism to ensure the integrity of this data.* After initial installation, the TOE obtains its remediation data updates either from manual entry by an authorized user or by remote download from the McAfee® Hercules® VFlash server. Since all McAfee® Hercules® users are subject to the I&A mechanisms of the product (FIA_UAU.2, FIA_UID.2) it follows that only authorized and identified users may manually create remediation data. The product also enforces the IMPORT_SFP information flow security functional policy (FDP_IFC.1 (1), FDP_IFF.1 (1), FDP_ITC.1) when importing remediation data from the V Flash server. This ensures that the remediation data is obtained from a trusted source. The TOE maintains an audit record of import sessions (FAU_GEN.1, FAU_GEN.2) so that it is possible to confirm that the product has current, accurate and valid remediation data.
O.SCANDATA	*The TOE must ensure that its scanner data is obtained from trusted sources and must provide a mechanism to ensure the confidentiality and integrity of this data.* The TOE enforces the IMPORT_SFP information flow control security functional policy (FDP_ITC.1) to ensure that only trusted scanner data is imported by the TOE. Once under the control of the TOE, the scanner data may only be accessed by authorized TOE users (FMT_MTD.1). This ensures the confidentiality and integrity of the data. The audit trail records the details of scanner data import sessions (FAU_GEN.1, FAU_GEN.2).
O.USERDATA	*The TOE must ensure that exported user data is secure.* The TOE enforces EXCHANGE_SFP data exchange information flow control security functional policy (FDP_IFC.1 (2), FDP_IFF.1 (2), FDP_ETC.1).
OE.AUTHUSER	*Only authorized personnel are permitted physical access to the TOE.* The environment is assumed to restrict physical access to the TOE (A.PHYSICAL), which provides physical security and restricts physical access to authorized personnel.
OE.BACKUP	*Good backup and recovery procedures for the TOE must be in place.* The environment is assumed to provide good backup and recovery procedures (A.BACKUP).
OE.DOMAIN	*The host operating system will provide domain separation and ensure that the TOE cannot be tampered with.*

	The Environment shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects (FPT_SEP.1€).
OE.GOODOS	*Those portions of the client operating system required for the correct operation of the TOE must function correctly.*
	The environment is assumed to be properly configured and may therefore be trusted to function correctly for those OS functions required by the TOE component that is installed on the client machine (A.GOODOS). In addition, the environment supports and monitors the correct functioning of the TOE by providing supplemental audit data generation (FAU_GEN.1€), a means of reviewing the supplemental audit data (FAU_SAR.1€), selective audit (FAU_SEL.1€), and reliable time stamps (FPT_STM.1€).
OE.GOODUSER	*Knowledgeable, non malicious users with system administrator privileges must be assigned to install, configure, administer, operate and maintain the TOE.*
	The environment is assumed to provide knowledgeable (A.KNOWLEDGE), non-hostile, users who follow all guidance documents (A.NOEVIL), and who have all necessary access to the device (A.TOEUSER).
OE.GUIDANCE	*The administrator(s) responsible for the TOE must ensure that the TOE is installed, configured, administered and operated in accordance with the guidance documents.*
	The environment is assumed to be securely configured and to remain in that configuration (A.CONFIG).
OE.PROTCOM	*The operating system and environment in which the TOE is to be installed must support the use of digital certificates for identification and authentication as well as SSL/SSH protocols to support the protection of communications between components.*
	The McAfee® Hercules® server can leverage the environment to protect data transferred to a client system using SSL for Windows® clients and OpenSSH for Unix clients. Digital certificates provide a two-way authentication between servers and clients (FDP_IFC.1€, FDP_IFF.1€). The TOE also protects its data from disclosure and modification while transmitting this data to the client systems (FPT_ITT.1€).
OE.SECURECOM	*The network on which the TOE resides must protect the confidentiality and integrity of information exchanged between the distributed elements of the TOE when client machines are initially installed remotely using the McAfee® Hercules® Client Management Service (CMS).*

The network on which the TOE resides is assumed to be protected (A.CMS). In addition, the environment protects the data transferred between separate parts of the TOE against disclosure and modification (FPT_ITT.1є).

8.3 SECURITY FUNCTIONAL REQUIREMENT DEPENDENCIES

Table 6 identifies the TOE and IT Environment Security Functional Requirements and their associated dependencies. It also indicates whether the TOE explicitly addresses each dependency. Notes are provided for those cases where the dependencies are satisfied by components which are hierarchical to the specified dependency.

Security Functional Requirement	**Dependencies**	**Dependency Satisfied**	**Notes**
FAU_GEN.1	FPT_STM.1	Yes	Satisfied by FPT_STM.1є.
FAU_GEN.2	FAU_GEN.1	Yes	
	FIA_UID.1	Yes	FIA_UID.2 is specified as a security functional requirement and FIA_UID.2 is hierarchical to FIA_UID.1.
FAU_SAR.1	FAU_GEN.1	Yes	
FAU_SAR.2	FAU_SAR.1	Yes	
FDP_ACC.2	FDP_ACF.1	Yes	
FDP_ACF.1	FDP_ACC.1	Yes	FDP_ACC.2 is specified as a security functional requirement and FDP_ACC.2 is hierarchical to FDP_ACC.1
	FMT_MSA.3	Yes	
FDP_ETC.1	FDP_ACC.1	Yes	FDP_ACC.2 is specified as a security functional requirement and FDP_ACC.2 is hierarchical to FDP_ACC.1
	FDP_IFC.1	Yes	Satisfied by FDP_IFC.1 (1), FDP_IFC.1 (2) and FDP_IFC.1 (3).
FDP_IFC.1 (1)	FDP_IFF.1	Yes	Satisfied by FDP_IFF.1 (1).
FDP_IFC.1 (2)	FDP_IFF.1	Yes	Satisfied by FDP_IFF.1 (2).
FDP_IFC.1 (3)	FDP_IFF.1	Yes	Satisfied by FDP_IFF.1 (3).

Security Functional Requirement	Dependencies	Dependency Satisfied	Notes
FDP_IFF.1 (1)	FDP_IFC.1	Yes	Satisfied by FDP_IFC.1 (1).
	FMT_MSA.3	Yes	
FDP_IFF.1 (2)	FDP_IFC.1	Yes	Satisfied by FDP_IFC.1 (2).
	FMT_MSA.3	Yes	
FDP_IFF.1 (3)	FDP_IFC.1	Yes	Satisfied by FDP_IFC.1 (3).
	FMT_MSA.3	Yes	
FDP_ ITC.1	FDP_IFC.1	Yes	Satisfied by FDP_IFC.1 (1), FDP_IFC.1 (2) and FDP_IFC.1 (3).
	FMT_MSA.3	Yes	
FDP_ROL.1	FDP_IFC.1	Yes	Satisfied by FDP_IFC.1 (1), FDP_IFC.1 (2) and FDP_IFC.1 (3).
FIA_ATD.1	None	N/A	
FIA_UAU.2	FIA_UID.1	Yes	FIA_UID.2 is specified as a security functional requirement and FIA_UID.2 is hierarchical to FIA_UID.1.
FIA_UAU.6	None	N/A	
FIA_UID.2	None	N/A	
FIA_USB.1	FIA_ATD.1	Yes	
FMT_MOF.1	FMT_SMR.1	Yes	
	FMT_SMF.1	Yes	
FMT_MSA.1 (1)	FDP_IFC.1	Yes	Satisfied by FDP_IFC.1 (1).
	FMT_SMF.1	Yes	
	FMT_SMR.1	Yes	
FMT_MSA.1 (2)	FDP_IFC.1	Yes	Satisfied by FDP_IFC.1 (2).
	FMT_SMF.1	Yes	
	FMT_SMR.1	Yes	
FMT_MSA.1 (3)	FDP_IFC.1	Yes	Satisfied by FDP_IFC.1 (3).
	FMT_SMF.1	Yes	
	FMT_SMR.1	Yes	

Security Functional Requirement	Dependencies	Dependency Satisfied	Notes
FMT_ MSA.3	FMT_MSA.1	Yes	Satisfied by FMT_MSA.1 (1), FMT_MSA.1 (2) and FMT_MSA.1 (3).
	FMT_SMR.1	Yes	
FMT_MTD.1	FMT_SMF.1	Yes	
	FMT_SMR.1	Yes	
FMT_REV.1	FMT_SMR.1	Yes	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	Yes	FIA_UID.2 is specified as a security functional requirement and FIA_UID.2 is hierarchical to FIA_UID.1.
FPT_RVM.1	None	N/A	
FAU_GEN.1є	FPT_STM.1	Yes	Satisfied by FPT_STM.1є.
FAU_SAR.1є	FAU_GEN.1	Yes	Satisfied by FAU_GEN.1є.
FAU_SEL.1є	FAU_GEN.1	Yes	Satisfied by FAU_GEN.1є.
	FMT_MTD.1	Yes	
FDP_IFC.1є	FDP_IFF.1	Yes	Satisfied by FDP_IFF.1є.
FDP_IFF.1є	FDP_IFC.1	Yes	Satisfied by FDP_IFC.1є.
	FMT_MSA.3	Yes	
FDP_ITT.1є	FDP_IFC.1	Yes	Satisfied by FDP_IFC.1є.
FPT_ITT.1є	None	N/A	
FPT_RVM.1є	None	N/A	
FPT_SEP.1є	None	N/A	
FPT_STM.1є	None	N/A	

Table 6 - Security Functional Requirement Dependencies

8.4 SECURITY ASSURANCE REQUIREMENT DEPENDENCIES

Security Functional Requirement	Dependencies	Dependency Satisfied	Notes
ACM_CAP.3	ACM_DVS.1	Yes	
ACM_SCP.1	ACM_CAP.3	Yes	
ADO_DEL.1	None	N/A	
ADO_IGS.1	AGD_ADM.1	Yes	
ADV_FSP.1	ADV_RCR.1	Yes	
ADV_HLD.2	ADV_FSP.1	Yes	
	ADV_RCR.1	Yes	
ADV_RCR.1	None	N/A	
AGD_ADM.1	ADV_FSP.1	Yes	
AGD_USR.1	ADV_FSP.1	Yes	
ALC_DVS.1	None	N/A	
ATE_COV.2	ADV_FSP.1	Yes	
	ATE_FUN.1	Yes	
ATE_DPT.1	ADV_HLD.1	Yes	ADV_HLD.2 is specified as a security assurance requirement and ADV_HLD.2 is hierarchical to ADV_HLD.1.
	ATE_FUN.1	Yes	
ATE_FUN.1	None	N/A	
ATE_IND.2	ADV_FSP.1	Yes	
	AGD_ADM.1	Yes	
	AGD_USR.1	Yes	
	ATE_FUN.1	Yes	
AVA_MSU.1	ADO_IGS.1	Yes	
	ADV_FSP.1	Yes	
	AGD_ADM.1	Yes	
	AGD_USR.1	Yes	
AVA_SOF.1	ADV_FSP.1	Yes	

Security Functional Requirement	Dependencies	Dependency Satisfied	Notes
	ADV_HLD.1	Yes	ADV_HLD.2 is specified as a security assurance requirement and ADV_HLD.2 is hierarchical to ADV_HLD.1.
AVA_VLA.1	ADV_FSP.1	Yes	
	ADV_HLD.1	Yes	ADV_HLD.2 is specified as a security assurance requirement and ADV_HLD.2 is hierarchical to ADV_HLD.1.
	AGD_ADM.1	Yes	
	AGD_USR.1	Yes	

Table 7 - Security Assurance Requirement Dependencies

8.5 TOE SUMMARY SPECIFICATION RATIONALE

Table 8 provides a bi-directional mapping of Security Functions to Security Functional Requirements, and is followed by a discussion of how each Security Functional Requirement is addressed by the corresponding Security Function.

	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.2	FDP_ACC.2	FDP_ACF.1	FDP_ETC.1	FDP_IFC.1 (1)	FDP_IFC.1 (2)	FDP_IFC.1 (3)	FDP_IFF.1 (1)	FDP_IFF.1 (2)	FDP_IFF.1 (3)	FDP_ITC.1	FDP_ROL.1	FIA_ATD.1	FIA_UAU.2	FIA_UAU.6	FIA_UID.2	FIA_USB.1	FMT_MOF.1	FMT_MSA.1 (1)	FMT_MSA.1 (2)	FMT_MSA.1 (3)	FMT_MSA.3	FMT_MTD.1	FMT_REV.1	FMT_SMF.1	FMT_SMR.1	FPT_RVM.1
F.ACCESS					X	X										X					X			X			X			
F.AGGVADATA																						X	X			X				
F.APPPROF																										X		X		
F.AUDIT	X	X	X	X																										
F.DISPCLIENT																										X				
F.DISPCLIENTSTATUS																										X				
F.DISPPROF																										X				
F.DISPREMSTATUS																										X				
F.DISPSIG																										X				
F.DISPVADATA																						X	X			X				
F.DISPVULN																										X				
F.EXPORTDATA							X		X			X																		
F.IAUSER											X	X					X	X	X	X		X	X	X	X	X	X		X	

	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.2	FDP_ACC.2	FDP_ACF.1	FDP_ETC.1	FDP_IFC.1 (1)	FDP_IFC.1 (2)	FDP_IFC.1 (3)	FDP_IFF.1 (1)	FDP_IFF.1 (2)	FDP_IFF.1 (3)	FDP_ITC.1	FDP_ROL.1	FIA_ATD.1	FIA_UAU.2	FIA_UAU.6	FIA_UID.2	FIA_USB.1	FMT_MOF.1	FMT_MSA.1 (1)	FMT_MSA.1 (2)	FMT_MSA.1 (3)	FMT_MSA.3	FMT_MTD.1	FMT_REV.1	FMT_SMF.1	FMT_SMR.1	FPT_RVM.1
F.IMPREMDATA								X	X		X	X		X								X	X		X					
F.IMPDATA								X	X		X	X		X								X	X		X					
F.IMPDEV								X	X		X	X		X								X	X		X					
F.MANAGEDATA														X								X	X		X			X		
F.MANAGEPROF																										X		X		
F.MANAGEROLES					X	X															X			X			X		X	
F.PUSHREM																												X		
F.PUSHPOLICY										X			X																	
F.REMCLIENT																												X		
F.REMPOLICY																												X		
F.REPREMSTATUS			X																											
F.ROLLBACK															X													X		
F.RVM																														X
F.SCHEDREM																									X		X			

Table 8 - Mapping of Security Functions to Security Functional Requirements

FAU_GEN.1 *Audit data generation*

The audit function of the TOE collects (F.AUDIT) and stores audit data for actions which are specific to the TOE (scanner data import, remediation data import, client remediations). In addition, the operating system audit trail retains audit records related to the identification and authorization of users, the start up and shut down of the TOE and the start up and shut down of the OS audit mechanism.

FAU_GEN.2 *User Identity Association*

The audit function of the TOE collects (F.AUDIT) and stores the identity of the user who caused an auditable event.

FAU_SAR.1 *Audit review*

The TOE includes a comprehensive HMI (McAfee® Hercules® Administrator Console) with extensive display and reporting features (F.REPREMSTATUS) which permit all authorized users with the ability to review, scan, analyze and interpret the audit trail recorded by the TOE (F.AUDIT).

FAU_SAR.2 *Restricted audit review*

The TOE HMI (McAfee® Hercules® Administrator Console) provides authorized users with the ability to view audit information (F.AUDIT).

FDP_ACC.2 *Complete access control*

The TOE incorporates access control (F.ACCESS). Authorized users are subject to the ADIMN_ACCESS SFP access control security functional policy for the management of role-based access control. Users are assigned to roles that allow specific administrative functionality on the McAfee® Hercules® Server (F.MANAGEROLES).

FDP_ACF.1 *Security attribute based access control*

The TOE incorporates role-based access control (F.ACCESS). Authorized users are subject to the ADIMN_ACCESS SFP access control security functional policy for the management of role-based access control. Users are assigned to roles that allow specific administrative functionality on the McAfee® Hercules® Server (F.MANAGEROLES).

FDP_ETC.1 *Export of user data without security attributes*

The TOE exports (F.EXPORTDATA) user data for backup or transfer to another McAfee® Hercules® Server.

FDP_IFC.1 *Subset information flow control (1)*

Each McAfee® Hercules® Server also enforces the IMPORT_SFP information flow control security functional policy when importing both vulnerability scan data (F.IMPDATA), vulnerability remediation data (F.IMPREMDATA) and device identifier data (F.IMPDEV).

FDP_IFC.1 *Subset information flow control (2)*

Each McAfee® Hercules® Server enforces the EXCHANGE_SFP information flow control security functional policy when exporting data files to the same or different McAfee® Hercules® Server (F.EXPORTDATA) and subsequent import of remediation data (F.IMPREMDATA), vulnerability scan data (F.IMPDATA) and device identifier data (F.IMPDEV).

FDP_IFC.1 *Subset information flow control (3)*

Each McAfee® Hercules® Server enforces the CONNECT_SFP information flow control security functional policy which restricts the ability of client machines to communicate over the network until remediation data has been pushed to the device (F.PUSHPOLICY).

FDP_IFF.1 *Simple security attributes (1)*

The TOE uses the IMPORT_SFP information flow control security functional policy to govern the import of vulnerability scan information (F.IMPDATA), vulnerability remediation data (F.IMPREMDATA) and device identifier data (F.IMPDEV) from trusted external sources by an authorized TOE user (F.IAUSER).

FDP_IFF.1 *Simple security attributes (2)*

The TOE uses the EXCHANGE_SFP information flow control security functional policy to govern the exchange of data between McAfee® Hercules® Servers. This policy states that the server must identify and authenticate the user before allowing them to export data files (F.EXPORTDATA) and the subsequent import of remediation data (F.IMPREMDATA), vulnerability scan data (F.IMPDATA) and device identifier data (F.IMPDEV) from trusted external sources by an authorized TOE user (F.IAUSER).

FDP_IFF.1 *Simple security attributes (3)*

The TOE uses the CONNECT_SFP information flow control security functional policy to govern the exchange of data between a McAfee® Hercules® Server and one of its client systems. This policy states that the server must identify and authenticate the client before allowing the client machines to communicate over the network until remediation data has been pushed to the device (F.PUSHPOLICY).

FDP_ITC.1 *Import of user data without security attributes*

When importing vulnerability scan data (F.IMPDATA) or vulnerability remediation data (F.IMPREMDATA) or device identifier data (F.IMPDEV) from trusted external sources, the TOE ignores any security attributes associated with the external data and instead applies the properties specified by the authorized TOE user (F.MANAGEDATA) to the imported data.

FDP_ROL.1 *Basic Rollback*

The TOE allows the rollback (F.ROLLBACK) of specific automatic vulnerability remediations under specified circumstances.

FIA_ATD.1 *User attribute definition*

The TOE restricts access through the use of user identification and authentication. (F.ACCESS).

FIA_UAU.2 *User authentication before any action*

The user identification and authentication mechanisms used by the TOE (F.IAUSER), require complete and successful authentication before allowing any action to be performed.

FIA_UAU.6 *Re-authenticating*

Authorized McAfee® Hercules® users will be re-authenticated when changing McAfee® Hercules® Server (F.IAUSER).

FIA_UID.2 *User identification before any action*

The user identification and authentication mechanisms used by the TOE (F.IAUSER), require successful identification either of the individual user or the requesting system, before allowing any action to be performed.

FIA_USB.1 *User-subject binding*

The McAfee® Hercules® Administrator Console executes user identification with every request (F.IAUSER).

FMT_MOF.1 *Management of security functions behaviour*

Authorized users are subject to the ADIMN_ACCESS SFP access control security functional policy for the management of role-based access control (F.ACCESS). The TOE provides the capability to create custom roles to which individual users and groups of users may be assigned (F.MANAGEROLES).

FMT_MSA.1 *Management of Security Attributes (1)*

Only authorized McAfee® Hercules® users have access to the functions of the TOE (F.IAUSER). These users are subject to the SERVER_SFP information flow control security functional policy for the import of vulnerability scan data (F.IMPDATA), vulnerability remediation data (F.IMPREMDATA) and device identifier data (F.IMPDEV). Authorized users may also display the imported vulnerability data (F.DISPVADATA) and aggregate vulnerability information from multiple scans into a unified vulnerability picture for client systems (F.AGGVADATA). Authorized TOE users have the ability to manipulate all of the vulnerability and remediation data held by the TOE (F.MANAGEDATA).

FMT_MSA.1 *Management of Security Attributes (2)*

Only authorized McAfee® Hercules® users have access to the functions of the TOE (F.IAUSER). These users are subject to the IMPORT_SFP information flow control security functional policy for the import of vulnerability scan data (F.IMPDATA), vulnerability remediation data (F.IMPREMDATA) and device identifier data (F.IMPDEV). Authorized users may also display the imported vulnerability data (F.DISPVADATA) and aggregate vulnerability information from multiple scans into a unified vulnerability picture for client systems (F.AGGVADATA). Authorized TOE users have the ability to manipulate all of the vulnerability and remediation data held by the TOE (F.MANAGEDATA).

FMT_MSA.1 *Management of Security Attributes (3)*

Only authorized McAfee® Hercules® users have access to the functions of the TOE (F.IAUSER). These users are subject to the ADMIN_ACCESS_SFP information flow control security functional policy which incorporates a role-based access control capability (F.ACCESS). The TOE provides the capability to create custom roles to which individual users and groups of users may be assigned (F.MANAGEROLES).

FMT_MSA.3 *Static attribute initialization*

Only authorized McAfee® Hercules® users have access to the TOE for the purposes of initializing security attributes (F.IAUSER). The security attributes are used for mutual identification and authentication between the McAfee® Hercules® Server and the client

machines. The McAfee® Hercules® users are subject to the IMPORT_SFP information flow control security function policy for the import of vulnerability scan data (F.IMPDATA), vulnerability remediation data (F.IMPREMDATA) and device identifier data (F.IMPDEV). Authorized TOE users may specify alternative initial values to override default values when data is imported (F.MANAGEDATA).

FMT_MTD.1 *Management of TSF Data*

Only authorized McAfee® Hercules® users have access to the TOE (F.IAUSER). Only these users have the ability to manipulate (display, modify, delete, aggregate) vulnerability data (F.AGGVADATA, F.DISPVADATA, F.DISPSIG) remediation data (F.DISPPROF, F.MANAGEPROF, F.APPPROF) and client system vulnerability and remediation data (F.DISPVULN, F.DISPCLIENT, F.DISPCLIENTSTATUS, F.DISPREMSTATUS, F.SCHEDREM).

FMT_REV.1 *Revocation*

Only authorized McAfee® Hercules® users have access to the TOE (F.IAUSER). These users are subject to the ADMIN_ACCESS_SFP information flow control security functional policy which incorporates a role-based access control capability (F.ACCESS). The TOE provides the capability to restrict access to various tasks by removing those privileges to the use of specific functions (F.MANAGEROLES).

FMT_SMF.1 *Specification of Management Functions*

The TOE allows authorized users complete control of the vulnerability and remediation data for all client systems (F.MANAGEDATA). Users may create, edit and approve remediation profiles for client systems or groups of client systems (F.MANAGEPROF, F.APPPROF). Users may also schedule automatic remediation activity for client systems or groups of client systems (F.SCHEDREM, F.PUSHREM, and F.REMPOLICY). This allows users to remove specific vulnerabilities from specific client systems (F.REMCLIENT). If desired it is also possible is specific circumstances to roll back a previously applied remediation (F.ROLLBACK).

FMT_SMR.1 *Security Roles*

By default, the TOE assigns the McAfee® Hercules® System Administrator role to the user name that installed the McAfee® Hercules® Server. Members of this role have access to all of the functionality of the TOE and can perform any of the pre-defined tasks. Additionally only individuals authorized as administrators by the underlying operating system are recognized as members of the McAfee® Hercules® user role (F.IAUSER). The TOE provides the capability to create custom roles to which individual users and groups of users may be assigned (F.MANAGEROLES). The ability to use specific features of the TOE such as the creation of user defined vulnerabilities may be assigned to custom roles.

FPT_RVM.1 *Non-bypassability of the TSP*

The TOE (and supporting host operating system) ensures that the TSP enforcement functions are invoked and successful before any function within the TSC is activated (F.RVM).

8.6 TOE ASSURANCE MEASURES RATIONALE

The McAfee® Hercules® product is designed to protect the TOE and its data from network attacks, to limit the system's use of network interfaces to those specified by the user, and to be simple enough for a knowledgeable system administrator to use. An assurance level of EAL 3, Methodically Tested and Checked, was selected as the threat to security is considered to be unsophisticated network attackers, and the data to be protected consists primarily of user-private data and system resources. An evaluation at this level provides a moderate level of independently assured security via a thorough investigation of the TOE and its development.

Table 9 provides a bi-directional mapping of Assurance Measures to Assurance Requirements, and is followed by a short discussion of how the Assurance Requirements are addressed by the corresponding Assurance Measures.

	ACM_CAP.3	ACM_SCP.1	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.2	ADV_RCR.1	AGC_ADM.1	AGD_USR.1	ALC_DVS.1	ATE_COV.2	ATE_DPT.1	ATE_FUN.1	ATE_IND.2	AVA_MSU.1	AVA_SOF.1	AVA_VLA.1
M.AUTH	X																
M.CONFIG	X	X															
M.DELIVER			X														
M.DESIGN					X	X	X										
M.DEVELOP										X							
M.DOCS								X	X						X		
M.ID	X																
M.SETUP				X													
M.TEST											X	X	X	X			
M.VULNER																X	X

Table 9 - Mapping of Assurance Measures to Assurance Requirements

ACM_CAP.3 Authorisation Controls

Assurance Measure M.ID ensures that the TOE is uniquely identified and labelled with its identity. Assurance Measure M.CONFIG ensures that the TOE includes a configuration item list. Assurance Measure M.AUTH ensures that only authorised changes are permitted to the TOE. These measures combine to satisfy the requirements of ACM_CAP.3.

ACM_SCP.1 TOE CM Coverage

Assurance Measure M.CONFIG ensures that the TOE includes a configuration item list. The contents of this list ensure that the requirements of ACM_SCP.1 are met.

ADO_DEL.1 Delivery Procedures

Assurance Measure M.DELIVER ensures that the TOE includes documentation describing the delivery procedures for the TOE. This measure satisfies the requirements of ADO_DEL.1.

ADO_IGS.1 Installation, Generation and Start-up Procedures

Assurance Measure M.SETUP ensures that the TOE includes documentation describing its secure installation, generation and start-up. This measure satisfies the requirements of ADO_IGS.1.

ADV_FSP.1 Informal Functional Specification

Assurance Measure M.DESIGN ensures that the TOE design documentation includes an informal function specification. This measure satisfies the requirements of ADV_FSP.1.

ADV_HLD.2 Security Enforcing High Level Design

Assurance Measure M.DESIGN ensures that the TOE design documentation includes an informal high level design which includes; a description of the TSF in terms of subsystems, a description of the purpose and method of use of all interfaces to the subsystems and a description of the separation of the TOE into TSP enforcing and other subsystems. These features satisfy the requirements of ADV_HLD.2.

ADV_RCR.1 Informal Correspondence Demonstration

Assurance Measure M.DESIGN ensures that the TOE design documentation includes an informal correspondence demonstration between the TOE Summary Specification, the Functional Specification and the High Level Design. This measure satisfies the requirements of ADV_RCR.1.

AGD_ADM.1 Administrator Guidance

Assurance Measure M.DOCS ensures that the TOE documentation includes a user manual and online help system. Since all users of the TOE are also administrators (refer to assumption A.TOEUSER), this documentation acts as both User and Administrator guidance. This measure satisfies the requirements of AGD_ADM.1.

AGD_USR.1 User Guidance

Assurance Measure M.DOCS ensures that the TOE documentation includes a user manual and online help system. This measure satisfies the requirements of AGD_USR.1.

ALC_DVS.1 Identification of Security Measures

Assurance Measure M.DEVELOP ensures that the TOE documentation includes a description of the security measures for the TOE development environment. This measure satisfies the requirements of ALC_DVS.1.

ATE_COV.2 Analysis of Coverage

Assurance Measure M.TEST ensures that the TOE test documentation includes sufficient evidence to confirm that the developer has systematically tested the TOE against its functional specification and high level design. This measure satisfies the requirements of ATE_COV.2.

ATE_DPT.1 Testing: High Level Design

Assurance Measure M.TEST ensures that the TOE test documentation includes sufficient evidence to demonstrate that the TSF operates in accordance with its high level design. This measure satisfies the requirements of ATE_DPT.1.

ATE_FUN.1 Functional Testing

Assurance Measure M.TEST ensures that the TOE test documentation is sufficient to determine that the developer has functionally tested all TOE security functions. This measure satisfies the requirements of ATE_FUN.1.

ATE_IND.2 Independent Testing – Sample

Assurance Measure M.TEST ensures that the TOE test documentation is sufficient for the evaluator to repeat a sample of the developers functional testing in order to confirm the test results as well as develop independent tests of the TOE security functions. This measure satisfies the requirements of ATE_IND.2.

AVA_MSU.1 Examination of Guidance

Assurance Measure M.DOCS ensures that the TOE documentation includes guidance documentation. This documentation may be examined for misleading, unreasonable and conflicting guidance. This measure satisfies the requirements for AVA_MSU.1.

AVA_SOF.1 Strength of TOE Security Function Evaluation

Assurance Measure M.VULNER ensures that the TOE vulnerability analysis documentation includes a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim. This measure satisfies the requirements of AVA_SOF.1.

AVA_VLA.1 Developer Vulnerability Analysis

Assurance Measure M.VULNER ensures that the TOE vulnerability analysis documentation includes an analysis of obvious ways in which a user can violate the TOE security policies along with the disposition of these obvious vulnerabilities. This measure satisfies the requirements of AVA_VLA.1.