GuardianEdge

GuardianEdge Data Protection Framework 9.0.1 with GuardianEdge Hard Disk Encryption 9.0.1 and GuardianEdge Removable Storage Encryption 3.0.1

Security Target

Version 2.01

Common Criteria EAL4 augmented with ALC_FLR.3

October 20, 2008

475 Brannan Street, Suite 400, San Francisco CA 94107-5421 800-440-0419 415-683-2200 Fax 415-683-2400

www.guardianedge.com

Contents

1.0 Introduction 5
1.1 Identification 5
1.2 ST Overview 5
1.3 Common Criteria Conformance 5
1.4 Document Organization 6
1.5 Document Conventions 6
2.0 TOE Description 7
2.1 Product Description 7
2.2 TOE Physical Boundary and Scope of Evaluation 8
2.3 Logical Boundary 10
2.3.1 Evaluated Security Features 10
2.3.2 Evaluated Configuration 12
3.0 TOE Security Environment 13
3.1 Assumptions 13
3.2 Threats 14
3.3 Organizational Security Policies 14
4.0 Security Objectives 14
4.1 Security Objectives for the TOE 14
4.2 Security Objectives for the Environment 15
4.2.1 IT Environmental Security Objectives 15
4.2.2 Non-IT Environmental Security Objectives 16
5.0 IT Security Requirements 16
5.1 TOE Security Requirements 16
5.1.1 TOE Security Functional Requirements 16
5.1.2 TOE Security Assurance Requirements 25
5.1.3 Strength of Function 25
5.2 Security Requirements for the IT Environment 26
6.0 TOE Summary Specification 27

6.1 Security Audit 28
6.2 Cryptographic Support 30
6.2.1 Hard disk encryption 31
6.2.2 Removable Storage Encryption 32
6.3 Data Protection 32
6.4 Identification and Authentication 33
6.5 Security Management 35
6.6 TOE Protection 37
6.7 Access Banner 41
6.8 SOF Claims 41
6.9 TOE Assurance Measures 41
7.0 Protection Profile Claims 47
8.0 Rationale 47
8.1 Security Objectives Rationale 47
8.1.1 Security Objectives Rationale for Threats 47
8.1.2 Assumptions Addressed 51
8.1.3 All Objectives covered 52
8.2 Security Requirements Rationale 53
8.2.1 Assurance Rationale 60
8.2.2 Explicitly Stated Requirements Rationale 60
8.2.3 Dependencies 61
8.2.4 Rationale for Dependencies Not Satisfied 63
8.2.5 Rationale that IT Security Requirements are Internally Consistent 64
8.3 TOE Summary Specification Rationale 66
8.3.1 IT Security Functions Rationale 66
8.3.2 Rationale for Assurance Measures to Security Assurance Requirements 70
8.4 Strength of Function Claims 70
8.5 List of Acronyms 71
9.0 Glossary 71
10.0 References 75

Tables

Table 1 Identification Summary 5

Table 2 TOE SFRs.... 17

Table 3 Management of TSF Data in the TOE.... 23

Table 4 Functional Components for the IT environment 26

Table 5 Mapping TOE Security Functions and Requirements 27

Table 6 Audit Record Information 29

Table 7 Authentication methods, authentication keys and cryptographic operations.... 32

Table 8 Subsystems and Processing Environments.... 38

Table 9 Mapping of Assurance Requirements to Assurance Measures.... 42

Table 10 Threats, Objectives, and Rationale 48

Table 11 Mapping of Assumptions to Objectives 51

Table 12 Reverse Mapping of Security Objectives to Threats/Assumptions 52

Table 13 Mapping of Security Objectives to Security Functional Requirements 53

Table 14 Reverse mapping of SFRs to Security Objectives.... 58

Table 15 Rationale for Explicit Requirements 60

Table 16 TOE Dependencies Satisfied.... 61

Table 17 IT Environment Dependencies are Satisfied 63

Table 18 Dependencies Not Satisfied.... 63

Table 19 Management Specifications Complete 64

Table 20 Mapping SFRs to TOE Summary Specification Rationale 66

1.0 Introduction

1.1 Identification

The following table provides the required identification of the GuardianEdge Data Protection Framework 9.0.1 with GuardianEdge Hard Disk Encryption 9.0.1 and GuardianEdge Removable Storage Encryption 3.0.1 Security Target.

Table 1 Identification Summary

Title	GuardianEdge Data Protection Framework 9.0.1 with GuardianEdge Hard Disk Encryption 9.0.1 and GuardianEdge Removable Storage Encryption 3.0.1 Security Target
ST Version	2.01
Vendor	GuardianEdge, San Francisco, CA
TOE	GuardianEdge Data Protection Framework 9.0.1 with GuardianEdge Hard Disk Encryption 9.0.1 and GuardianEdge Removable Storage Encryption 3.0.1
Assurance Level	EAL4 augmented with ALC_FLR.3
Protection Profile Conformance	None
FIPS 140-2 Status	Level 1, Validated crypto module, Certificate No. 515
Encryption Library	Encryption Plus Cryptographic Library 1.0.4

1.2 ST Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for the GuardianEdge Data Protection Framework, GuardianEdge Hard Disk Encryption, and GuardianEdge Removable Storage Encryption (collectively referred to as the “GuardianEdge Platform”). The GuardianEdge Platform provides transparent encryption services for hard disks and removable storage devices on computers running Windows XP. It employs full disk encryption, pre-Windows authentication, and on-the-fly disk decryption/encryption at the device driver level to provide complete protection of data on Windows-based notebook and desktop systems. It also protects information on removable storage devices such as USB flash drives.

1.3 Common Criteria Conformance

This document conforms to the Common Criteria (CC) for Information Technology (IT) Security Evaluation, Version 2.3, dated August 2005 (International Standard—ISO/IEC 15408). The TOE is Part 2 extended, Part 3 conformant, and Evaluation Assurance Level (EAL) 4 conformant.

1.4 Document Organization

Section 1, “Introduction,” identifies the ST and presents the overview. This section also includes document conventions and organization, the CC conformance statement, and a list of CC and product-specific acronyms.

Section 2, “TOE Description,” defines the product type, scope, and boundaries.

Section 3, “TOE Security Environment” cites assumptions regarding the TOE's intended use and environment, and identifies potential threats.

Section 4, “Security Objectives,” identifies the TOE security objectives and describes how they would meet a security problem.

Section 5, “Security Requirements,” addresses Security Functional Requirements, Security Requirements for the IT environment, and the Security Assurance Requirements.

Section 6, “TOE Summary Specification,” provides a summary of the IT Security Functions and Assurance Measures.

Section 7, “Protection of Profile Claims,” This section is non-applicable. ST does not include PP conformance.

Section 8, “Rationale,” provides evidence confirming that the ST contains a complete, cohesive set of requirements, and that a TOE in conformance with the requirements would provide effective IT security countermeasures within the security environment of the evaluated configuration. Three types of rationale are presented: Security Objective, Security Requirement, and TOE Summary Specification.

“Glossary,” defines the terms used in this document.

“References,” provides various references for technical standards.

1.5 Document Conventions

Iterations are identified by parentheses, for example FIA_UAU.2(1).

Assignment and selection operations are identified by bold, italicized text within brackets:
[***assignment*** or ***selection value***].

Refinements are identified by **bold text**.

Explicitly stated requirements are identified by the tag EXP, for example FPT_SEP_ENV_EXP.1.

2.0 TOE Description

2.1 Product Description

The GuardianEdge Platform provides transparent encryption services for hard disks and removable storage devices on computers running Windows XP. It employs full disk encryption, pre-boot authentication, and on-the-fly disk decryption/encryption at the device driver level to provide complete protection of data on Windows-based notebook and desktop systems. It also protects information on removable storage devices such as USB flash drives.

The GuardianEdge Platform is intended for use in computing environments where there is a potential for attackers possessing a moderate attack potential.

The GuardianEdge Platform protects data at rest on the hard disk and on removable devices from unauthorized access. The GuardianEdge Platform uses its own FIPS 140-2 validated cryptographic library to perform the cryptographic operations necessary to protect data, support authentication, and self-protect itself against tampering or bypass. The product uses Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode with 256-bit keys to perform bulk encryption on administrator-specified partitions of hard disks and removable storage devices on a Client Computer.

During the initial encryption process, the GuardianEdge Platform encrypts all data on the hard disk except its own set of files that runs in the pre-Windows environment: the GuardianEdge Pre-Boot Authentication component (GPBA). The GPBA is called by the BIOS and creates its own pre-Windows environment to perform the authentication and subsequent decryption to start the operating system. The product's scope of protection includes the Windows operating system files, swap files, hibernation files, paging files, executables and all data stored on the hard disk. For removable storage devices encryption happens on a per file basis; the initial encryption of a given file happens when that file is written to the removable device.

The product's pre-Windows authentication function prevents Windows from loading until a registered GuardianEdge user successfully authenticates. Once authenticated, users gain access to Windows and to all applications and data, subject to the operating and application access controls. In a multi-user environment, the GuardianEdge Platform provides access control for the initial user starting the computer; subsequent users are authenticated by the operating system. The product offers several authentication options, including an "Advanced Authentication" module that supports tokens utilizing PKCS #11 access and X.509 certificates, and a Single Sign-On mechanism that synchronizes the GuardianEdge password with a Windows password. The password-based mechanism and its supporting authentication failure and password complexity requirements are the evaluated options.

For data on hard disk, following pre-boot authentication, the GuardianEdge Platform makes the data available transparently to users and applications via the operating system by performing on-the-fly decryption at the device driver level. The data is then re-encrypted when written back to disk. By providing the cryptographic services at the device driver level, the GuardianEdge Platform is able to protect all the data and function automatically and transparently—this ensures that the user's usual work flow is not disrupted and that security is always applied, rather than depending on users requesting the protection.

For data on removable storage devices, new files are automatically encrypted whenever they are written to the removable device. Depending on the configuration, existing plaintext files already on the removable storage device may be either left in plaintext or automatically encrypted. The evaluated configuration is for automatic encryption of pre-existing files to be disabled. Access is provided to encrypted files via on-the-fly decryption at the device driver level. Data for encrypted files is re-encrypted when data parts of that file are written back to disk. This ensures that the user's usual work flow is not disrupted, and that security of any files originating from the computer the removable storage device is attached to are encrypted automatically rather than depending on users requesting protection on a per file basis. In addition to AES bulk encryption, the GuardianEdge Platform uses Elliptic Curve Cryptography (ECC) asymmetric cryptographic algorithms to protect keys and authentication data and the SHA-1 hash function to verify the integrity of data, keys and code.

The administration of the GuardianEdge Platform follows the simplicity tenet for security architectures. A GuardianEdge Manager component, separate from the Client Computer, is used to create a set of installation files for the Client Computer. These files are copied to the Client Computer and when run install the Client Computer components, which provide the evaluated security functions. A console on the Client Computer provides an administrative interface to remove registered users and manage users' passwords. Registered users self-register during the logon process; Client Administrators are defined by the Policy Administrator during installation.

2.2 TOE Physical Boundary and Scope of Evaluation

The evaluated configuration of the GuardianEdge Platform comprises the software components listed below. The TOE includes all product components; however, in the evaluated configuration, some components do not provide any security functions and are therefore outside the scope of some assurance evaluation activities.

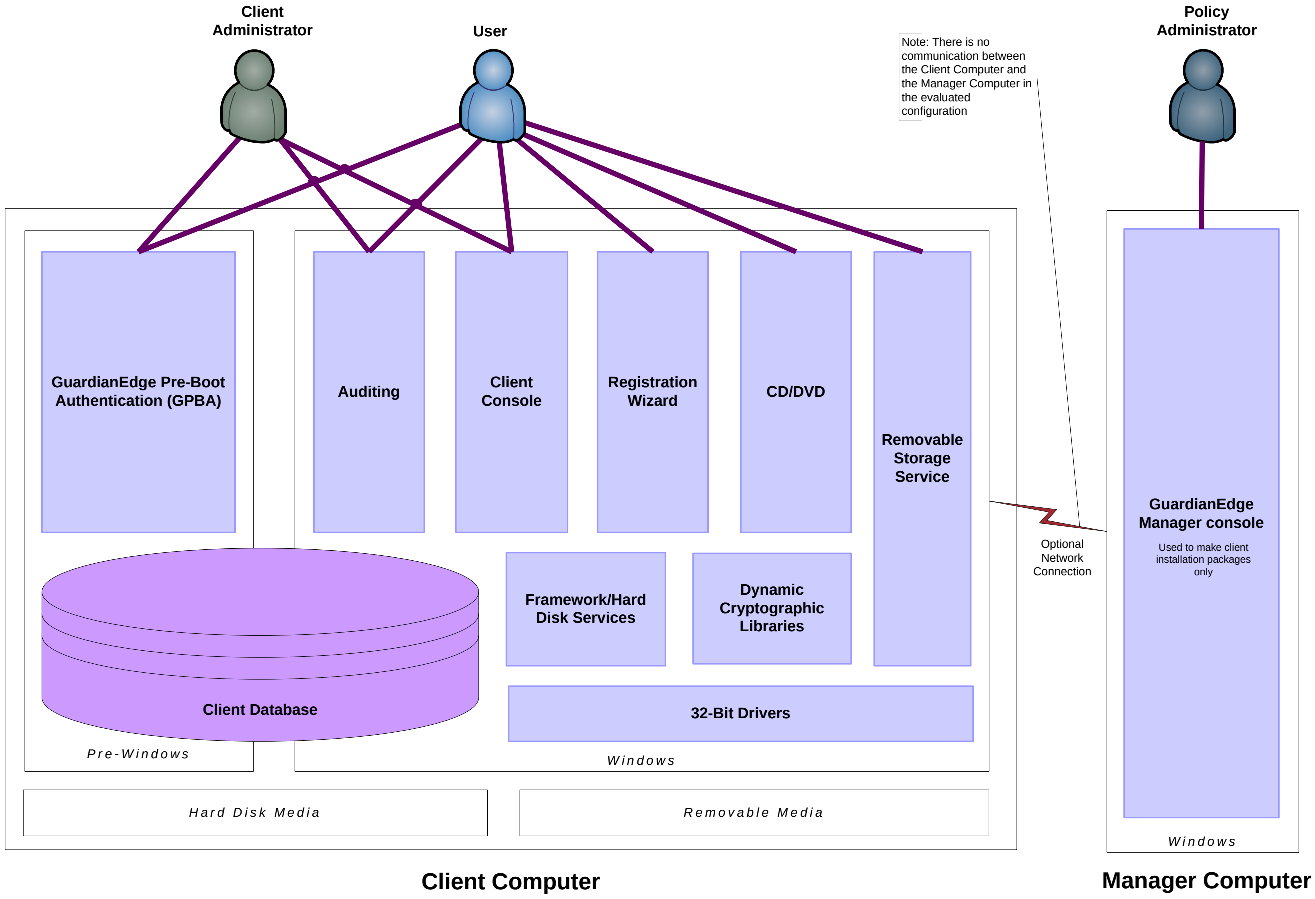
The following TOE components provide security functions in the evaluated configuration:

- *GuardianEdge Pre-Boot Authentication* operates in the pre-Windows environment to provide pre-Windows authentication, decryption services to start the operating system, self-tests, a master boot record to interface with the BIOS, and a file storage mechanism to support these functions, referred to as the GuardianEdge File System (GEFS).
- *GuardianEdge Hard Disk Encryption* includes a kernel-mode driver that performs on-the-fly decryption and encryption of data on the client hard disk.
- *GuardianEdge Removable Storage Encryption* includes a kernel-mode driver that performs decryption and encryption of data on the removable storage devices, and provides per-file password-based access control as required to decrypt files accessed on devices.
- *GuardianEdge Data Protection Framework* provides the cryptographic library and Client Console interface.

The following TOE components do not provide any security functions in the evaluated configuration:

- *The GuardianEdge Manager* is used by the Policy Administrator to create the Client Computer installation package, which is saved as a set of installation files on the GuardianEdge Manager computer. Various mechanisms can transfer the installation files from the management computer to the Client Computer. This component does not communicate with the TOE in the evaluated configuration. A network connection between the server and the client is not required. In the evaluated configuration, the GuardianEdge Manager is used in pre-installation only.

- *GuardianEdge Platform* support on the Client Computer.
- The optional *GuardianEdge Advanced Authentication 1.0.1* module, which supports secondary authentication devices.
- The optional *GuardianEdge Server*, provided with the product to support distributed administration.


Client Administrator
User
Note: There is no communication between the Client Computer and the Manager Computer in the evaluated configuration
Policy Administrator
GuardianEdge Pre-Boot Authentication (GPBA)
Auditing
Client Console
Registration Wizard
CD/DVD
Removable Storage Service
Client Database
Framework/Hard Disk Services
Dynamic Cryptographic Libraries
32-Bit Drivers
Pre-Windows
Windows
Hard Disk Media
Removable Media
Optional Network Connection
GuardianEdge Manager console
Used to make client installation packages only
Windows
Client Computer
Manager Computer

GuardianEdge Components and TOE Boundary

The TOE relies on the following IT environment components to support the evaluated security functions:

- The Client Computer including Windows XP Service Pack 3, x86 platform, hard disk and removable storage components and device drivers
- The Manager Computer including Windows 2003 Server, Service Pack 2, x86 platform with storage media for the client installation package files.

2.3 Logical Boundary

2.3.1 EVALUATED SECURITY FEATURES

The GuardianEdge Platform provides the security functions listed below. All security functions, and their associated security functional requirements (SFRs), are provided by the TOE components on the Client Computer. The GuardianEdge Manager is used for the installation process only and provides no security functions in the evaluated configuration. Support required for the TOE's IT environment is noted for each service.

1. Security Audit

   The TOE auditing service generates audit records into the Windows system event log of the Client Computer operating system. It captures security events related to use of the authentication mechanism, initial encryption activity, and the startup and shutdown of the TOE client. The TOE auditing service is automatically started with the start-up of the TOE client, and there is no interface to turn off the audit mechanism and no interface to change the security events being audited.

   The audit function requires the following support from the TOE's IT environment:

   - The OS to protect the Windows system event log to ensure it's protected from unauthorized deletion and modification.
   - The platform to provide reliable time when required to ensure the audit records have meaningful timestamps.
   - The OS to provide an interface to view the audit records in the Windows system event log.

2. Data Protection

   The TOE uses its FIPS140-2 cryptographic functions, described below, to ensure all data on the hard disk partitions, as designated by an administrator, is protected by encryption when not in use (i.e., at rest). Except for the GEFS files (to bootstrap the system), the encryption covers all the data on the selected hard disk partitions, including system files, e.g., Windows operating system files, registry, swap files, hibernation files, paging files. A per computer key is used to encrypt all data on the hard disk; this key is called the Workstation Encryption Key (WEK).

   The data protection function also ensures the data is available when requested and that both the encryption process (to protect the data when at rest) and the decryption process (to make the data available to registered users) is done transparently to the user, referred to as on-the-fly decryption/encryption. This transparent operation ensures enforcement and doesn't rely on users activating the function.

   Data on removable storage devices is encrypted on a per file basis. Files are automatically encrypted when written to the device. Encrypted files are decrypted when accessed and encrypted when written. Depending on the configuration, pre-existing plaintext files may be either automatically encrypted, or left as plaintext. The evaluated configuration is for pre-existing files to be left in plaintext. A per file key is used to encrypt files on removable storage devices; this key is called the File Encryption Key (FEK).

The data protection function requires the platform to be operating correctly, both in general for supporting the TOE processes and in particular for loading the TOE kernel-mode device drivers as configured in the installation process and processing the bits to ensure they pass through the TOE for the specified partitions.

3. Cryptographic Services

   The TOE includes cryptographic libraries that provide cryptographic support for the following security functions:

   Authentication process password check

   - Elliptic Curve Cryptography (ECC)
   - SHA-1

   New user registration

   - ECC
   - RNG

   Initial encryption and transparent decryption: AES in CBC mode.

   Self-tests and integrity checks: SHA-1 and CRC.

   The IT environment is only required to operate correctly to support the cryptographic services security function.

4. Identification and Authentication

   The TOE provides an identification and authentication (I&A) mechanism that requires all users to identify and authenticate themselves during the startup of the Client Computer, before the operating system is loaded and before users log on to their Windows accounts. This is referred to as pre-Windows authentication. In addition to the pre-Windows authentication requirement, the TOE also requires all users to log on again when accessing the GuardianEdge Client console.

   Supporting the password-based mechanism, the TOE obscures the password users enter on the TOE logon screens. It provides an authentication failure mechanism and password management options that defines parameters for acceptable passwords.

   The identification and authentication function depends on the operating system to identify and authenticate the Client Computer users after startup, and the platform to provide an accurate clock to measure one minute, the delay in the logon process for the authentication failure mechanism. As with all the security functions, it also requires the support provided as part of the Partial Self-Protection, described below, both in general and in particular for activating the TOE as part of the pre-Windows start-up process.

5. Security Management

   The TOE includes an administrative interface for Client Administrators to remove users, change passwords, and perform initial encryption on selected partitions. Registered users also use this interface to change their passwords. The GuardianEdge Platform in its evaluated configuration is designed to require minimum administration during normal operation. The Client Administrator, using the Client Console, is also able to verify the evaluated configuration settings. New users are added to the TOE through a self-registration process coordinated with the operating system logon for subsequent users after startup of the Client Computer.

The IT environment is required to operate correctly to support this security function.

6. Partial Self-Protection

   Working in concert with its platform the TOE provides a security architecture and security mechanisms to ensure the TSF cannot be bypassed, corrupted, or otherwise compromised.

   The TOE relies on its platform for domain separation of TSF processes, for non-bypassability, for access controls on file protections, and for correct operation of the BIOS and media driver data processing.

7. Access Banner

   The TOE displays an advisory warning access banner as part of its logon screen. The banner and warning are defined by the Policy Administrator during the installation process.

2.3.2 EVALUATED CONFIGURATION

Physical Components:

- Client platform: Windows XP, with Service Pack 3
- Manager console platform: Windows Server 2003, with Service Pack 2

Installation Configuration:

- GuardianEdge Server not installed.
- Client Monitor by checking in with platform—disabled.
- The two password recovery tools: Authenti-Check and One-Time Password—disabled.
- I&A optional mechanisms:

  Single Sign-On is disabled.

  Token authentication (“Advanced Authentication”) is disabled.

  Autologon is disabled.

  Grace restarts are disabled (set to zero).
- Initial Encryption configuration:

  Manual encrypt or decrypt partition enabled for Client Administrator only, not registered users.

  Unused sectors are included in the encryption.
- Removable Storage configuration:

  GuardianEdge Hard Disk Encryption is installed and all hard disk partitions of the protected operating system and associated user data partitions and swap partitions are encrypted.

  The GuardianEdge Removable Storage Access Utility is not used.

  Encryption policy set to “Encrypt New Files”.

The option to automatically encrypt pre-existing plaintext on removable devices is disabled.

The creation of self-extracting files is disabled.

Non-registered user support is disabled.

The access policy is set to read and write.

Encryption method is set to “password.”

Certificate (token and software based) encryption is disabled and/or not used.

Group Key feature is disabled.

No Master Certificate specified.

- Password policy: The specific password policy configuration for the evaluated configuration is provided in SOF Claims on page 41.
- A logon delay of one minute after a configured number of incorrect logons is enabled.

3.0 TOE Security Environment

3.1 Assumptions

The following is a list of assumptions regarding the security environment in which the TOE operates.

A.NET_ACC

It is assumed if the Client Computer is connected to a network, then remote users are required to log on to the Windows operating system to gain access, and that file sharing and other network services that don’t require a Windows logon and provide remote access to data stored on the Client Computer media are either disabled or there are appropriate network authentication and confidentiality services.

A.NO_EVIL

It is assumed that administrators are non-hostile, appropriately trained and follow all administrator guidance.

A.NO_MALWARE

It is assumed that environment procedures will ensure that the operating environment for the TOE runs only software, firmware, or hardware that has been approved by the security officer.

A.NO_UAT

It is assumed that users do not leave the GuardianEdge Client Computer unattended when they are logged on.

A.USERS

It is assumed that users will protect their authentication data.

A.NO_LOCAL_ADMIN

It is assumed that the user is not defined as a local administrator and has not been given local administrative privileges.

3.2 Threats

Threat agents are assumed to have an attack potential of medium for all threats. As a result, the TOE has been developed with the assumption that a potential attacker would have a medium level of expertise, access to a medium level of resources, and also possess a medium level of motivation.

The following threats are countered by the TOE:

T.IMPROPER_NOTICE

If proper notice of restricted use or other binding conditions is not provided, organizations may not be able to pursue legal sanctions. This would result in decreased effectiveness of administrative controls for protecting assets.

T.MASQUERADE

A malicious user or external IT entity may masquerade as another entity in order to gain unauthorized access to the Client Computer media assets.

T.TSF_COMPROMISE

A user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).

T.UNAUTHORIZED_MEDIA_ACCESS

An unauthorized user with physical access to the Client Computer may access assets stored on the hard disk and removable storage devices encrypted partitions by subverting the normal computer start-up processes or by removing the media from the computer.

T.UNIDENTIFIED_ACTIONS

The administrator may not have the ability to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach and hold persons accountable for their actions.

3.3 Organizational Security Policies

There are no organizational security policies governing the secure use of the TOE.

4.0 Security Objectives

4.1 Security Objectives for the TOE

O.AUDIT_GENERATION

The TOE will provide the capability to detect and create records of security relevant events associated with users.

O.CORRECT_ TSF_OPERATION

The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.

O.DISPLAY_BANNER

The TOE will display an advisory warning regarding use of the TOE.

O.MANAGE

The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.

O.MEDIASEC

The TSF must be able to protect the Client Computer media assets on the Client Administrator-specified hard disk partitions and removable storage devices, using encryption.

O.PARTIAL_SELF_PROTECTION

The TSF will maintain a domain for its own execution, and implement an architecture and mechanisms that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.

O.PARTIAL_TOE_ACCESS

The TSF will provide mechanisms that control user's logical access to the TOE Client Console and to the TOE mechanism that allows the Client Computer to start-up and make protected data available to the Client Computer users.

O.TRANSPARENT_ENFORCED_ACCESS

The TSF must be able to provide authorized users and system processes read and write access to the Client Computer encrypted partitions in a manner that is transparent to users. This ensures that the mechanism is always invoked and that the data is available to the system, authorized users, and applications and is encrypted when not in use and stored on the encrypted partitions.

4.2 Security Objectives for the Environment

4.2.1 IT ENVIRONMENTAL SECURITY OBJECTIVES

The following security objectives are part of the IT environment in which the TOE operates.

OE.AUDIT_SUPPORT

The IT environment will provide the capability to view audit information, and will protect the stored audit records from unauthorized modification and deletion, and will provide a timestamp for the audit records.

OE.PARTIAL_TOE_PROT

The TSF Environment shall provide virtual memory management, execution rings for executing user software and kernel processes to protect the TOE processes from interference and tampering, and file protection to prevent unauthorized access and modifications to TOE.

OE.TIMESTAMP

The TOE computing platform will provide reliable time.

OE.TOE_ENVIR_ACCESS

The IT environment will provide the capability to control users' logical access to the Client Computer after its startup.

4.2.2 NON-IT ENVIRONMENTAL SECURITY OBJECTIVES

This section contains policy- and personnel-related security objectives for the environment in which the TOE operates.

ON.NET_ACC

The environment procedures will ensure that the operational environment is suitable for the threats the TOE is designed to meet. For example, if the Client Computer is connected to a network, then remote users are required to log on to the Windows operating system to gain access, and that file sharing and other network services that don't require Windows logon and provide remote access to data stored on the Client Computer media are either disabled or there are appropriate network authentication and confidentiality services.

ON.NO_EVIL

The environment procedures will ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.

ON.NO_MALWARE

The environment procedures will ensure that the operating environment for the TOE runs only software, firmware, or hardware that has been approved by the security officer.

ON.NO_UAT

The environment procedures will ensure that users do not leave the GuardianEdge Client Computer unattended when they are logged on.

ON.USERS

The environment procedures will ensure that users will protect their authentication data.

ON.NO_LOCAL_ADMIN

The environment procedures will ensure that the user is not defined as a local administrator and has not been given local administrative privileges.

5.0 IT Security Requirements

5.1 TOE Security Requirements

5.1.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

The following requirements are taken from CC Part 2, except for those explicitly stated, which are denoted by _EXP in the SFR ID.

Table 2 TOE SFRs

Item	SFR ID	SFR Title
1.	FAU_GEN.1	Audit data generation
2.	FAU_GEN.2	User Identity Association
3.	FCS_CKM.1	Cryptographic key generation
4.	FCS_CKM.4	Cryptographic key destruction
5.	FCS_COP.1(1)	Cryptographic Operation (AES)
6.	FCS_COP.1(2)	Cryptographic Operation (ECC of UPC)
7.	FCS_COP.1(3)	Cryptographic Operation (RNG)
8.	FCS_COP.1(4)	Cryptographic Operation (Secure Hash)
9.	FCS_COP.1(5)	Cryptographic Operation (HMAC-SHA-1)
10.	FDP_IFC.2	Complete information flow control
11.	FDP_IFF.1	Simple security attributes
12.	FIA_AFL.1	Authentication failure handling
13.	FIA_SOS.1	Verification of secrets
14.	FIA_UAU.2	User authentication before any action (user access to Client Computer)
15.	FIA_UAU_TOE_EXP.2	User authentication before any action (Client console)
16.	FIA_UAU.7	Protected authentication feedback
17.	FIA_UID.2	User identification before any action (user access to Client Computer)
18.	FIA_UID_TOE_EXP.2	User identification before any action (Client console)
19.	FMT_MSA.1	Management of security attributes
20.	FMT_MSA.2	Secure security attributes
21.	FMT_MSA.3	Static attribute initialization
22.	FMT_MOF.1	Management of security functions behaviour
23.	FMT_MTD.1	Management of TSF data
24.	FMT_SMF.1	Specification of Management Functions
25.	FMT_SMR.1	Security roles
26.	FPT_RVM.1(1)	Non-bypassability of the TSP (TOE)
27.	FPT_SEP_TOE_EXP.1	TSF partial domain separation

Item	SFR ID	SFR Title
28.	FPT_TST.1	TSF testing
29.	FTA_TAB.1	Default TOE access banners

5.1.1.1 Security Audit (FAU)

FAU_GEN.1 *Audit data generation*

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

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

b) All auditable events for the [***not specified***] level of audit.

c) [

GEHD Successful and Unsuccessful logons.

GEHD Management actions of initial encryption process.

GEHD All changes to a user's authentication data.

GEHD Number of unsuccessful authentication attempts exceeded the maximum allowed.

GEHD Registered user added.

GEHD Registered user removed.

GERS Service started

GERS Service removed

GERS Service could not be removed

]

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 PP/ST, [***none***].

FAU_GEN.2 *User Identity Association*

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

5.1.1.2 Cryptographic Support (FCS)

FCS_CKM.1 *Cryptographic key generation*

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***ECES***] and specified cryptographic key sizes [***233-bit keys***] that meet the following: [***IEEE P1363 by vendor assertion***].

FCS_CKM.4 *Cryptographic key destruction*

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [***zeroization***] that meets the following: [***FIPS 140-2 Level 1, Key Destruction and overwriting for ECC keys***].

FCS_COP.1(1) *Cryptographic Operation (AES)*

FCS_COP.1(1).1 The TSF shall perform [***data encryption/decryption of media for initial encryption and on-the-fly decryption/encryption*]** in accordance with a specified cryptographic algorithm [***AES in CBC mode***] and cryptographic key sizes [***256-bit keys***] that meet the following: [***FIPS 197 and FIPS 140-2 level 1***].

FCS_COP.1(2) *Cryptographic Operation (ECC of UPC)*

FCS_COP.1(2).1 The TSF shall perform [***Elliptic Curve Cryptography encryption/decryption***] in accordance with a specified cryptographic algorithm [***ECES***] and cryptographic key sizes [***233-bit keys***] that meet the following: [***IEEE-P1363 by vendor assertion***].

Application Note: The ECES implementation was validated via source code review by domain experts.

FCS_COP.1(3) *Cryptographic Operation (RNG)*

FCS_COP.1(3).1 The TSF shall perform [***Random Number Generation***] in accordance with a specified cryptographic algorithm [***FIPS 186-2 appendix 3.1 with change notice 1***] and cryptographic key sizes [***N/A***] that meet the following: [***FIPS 186-2 and FIPS 140-2 level 1***].

FCS_COP.1(4) *Cryptographic Operation (Secure Hash)*

FCS_COP.1(4).1 The TSF shall perform [***Secure Hash***] in accordance with a specified cryptographic algorithm [***SHA-1***] and cryptographic key sizes [***N/A***] that meet the following: [***FIPS 180-1***].

FCS_COP.1(5) *Cryptographic Operation (Hash MAC)*

FCS_COP.1(5).1 The TSF shall perform [***MAC***] in accordance with a specified cryptographic algorithm [***HMAC-SHA-1***] and cryptographic key sizes [***160-bits***] that meet the following: [***FIPS 198***].

5.1.1.3 User Data Protection (FDP)

FDP_IFC.2 *Complete information flow control*

FDP_IFC.2.1 The TSF shall enforce the [***On-the-Fly Decryption/Encryption SFP***] on [

- ***subjects:***
  - ***all processes that access the client hard disk encrypted partitions and removable storage media***
  - ***the hard disk encrypted partitions and removable storage media***
- ***information: all]***

and all operations that cause that information to flow to and from subjects covered by the SFP.

Application Note: Encrypted partitions are the partitions on the hard disk that have been encrypted through the initial encryption process. This is done during installation or as a management function, as specified in FMT_MOF.1.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.

FDP_IFF.1 *Simple security attributes*

FDP_IFF.1.1 The TSF shall enforce the [***On-the-Fly Decryption/Encryption SFP***] based on the following types of subject and information security attributes: [

- ***subjects:***
  - ***all processes that access the client hard disk encrypted partitions and removable storage media encrypted files - read and write instructions;***
  - ***the hard disk encrypted partitions and removable storage media files - encrypted***
- ***information- file status (ENCRYPTED, or PLAINTEXT), relative sector address.]***

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [***none, all information flows through the TOE***].

FDP_IFF.1.3 The TSF shall enforce the [***none***].

FDP_IFF.1.4 The TSF shall provide the following [

a) For information flows where the subject is performing a write to a hard disk partition the TSF will encrypt the data using AES

(FCS_COP.1.1) in Cipher Block Chaining (CBC) mode using the WEK key and an Initialization Vector (IV) derived from the relative sector address with a PRNG.

b) For information flows where the subject is performing a read from a hard disk partition the TSF will decrypt the data using AES (FCS_COP.1.1) in Cipher Block Chaining (CBC) mode using the WEK key and an Initialization Vector (IV) derived from the relative sector address with a PRNG.

c) For information flows where the subject is performing a write to removal storage device media, if the file is decrypted, the TSF will encrypt the data using AES (FCS_COP.1.1) in Cipher Block Chaining (CBC) mode using the FEK key and an Initialization Vector (IV) derived from the block offset from the head of the encrypted data with a PRNG.

d) For information flows where the subject is performing a read from a removal storage device, if the file is encrypted, the TSF will decrypt the data sector using AES (FCS_COP.1.1) in Cipher Block Chaining (CBC) mode using the FEK key and an Initialization Vector (IV) derived from the block offset from the head of the encrypted data with a PRNG.

].

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: [***none***].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [***none***].

5.1.1.4 Identification and Authentication (FIA)

FIA_AFL.1 *Authentication failure handling*

FIA_AFL.1.1 The TSF shall detect when [a Policy Administrator–configurable positive integer defined at installation] unsuccessful authentication attempts occur related to [the unsuccessful authentication attempts for the current logon process].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [***delay the logon process for 60 seconds***.]

Application Note: Requirement element FIA_AFL.1.1 applies to FIA_UAU.2 and FIA_UID.2.

Application Note: The number of unsuccessful attempts before logon delay, as part of the password policy, is determined by the Policy Administrator at installation. This value is set to one in the evaluated configuration.

FIA_SOS.1 *Verification of secrets*

FIA_SOS.1. The TSF shall provide a mechanism to verify that secrets meet [the following password complexity rules defined by the Policy Administrator at installation:

- ***Minimum of eight total characters,***
- ***At least one non-alphanumeric character;***
- ***At least one UPPERCASE letter (A-Z and 32 accented uppercase characters); and***
- ***At least one digit (0-9).]***

Application Note: This requirement applies to both iterations of FIA_UAU.2 and FIA_UID.2.

FIA_UAU.2 *User authentication before any action (user access to Client Computer)*

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.

FIA_UAU_TOE_EXP.2 User authentication before any action (Client console)

FIA_UAU_TOE_EXP.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions from the Client Console interface on behalf of that user.

FIA_UAU.7 *Protected authentication feedback*

FIA_UAU.7.1 The TSF shall provide only [***display of bullet characters in place of characters typed***] to the user while authentication is in progress.

Application Note: This requirement applies to both iterations of FIA_UAU.2 and FIA_UID.2.

FIA_UID.2 *User identification before any action (user access to Client Computer)*

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.

FIA_UID_TOE_EXP.2 *User identification before any action (Client console)*

FIA_UID_TOE_EXP.2.1 The TSF shall require each user to identify itself again before allowing any other TSF-mediated actions from the Client Console interface on behalf of that user.

5.1.1.5 Security Management (FMT)

FMT_MOF.1 *Management of security functions behaviour*

FMT_MOF.1.1 The TSF shall restrict the ability to [***disable, enable***] the functions [

- ***On-the-fly decryption/encryption of a hard disk partition;***
- ***Terminal decryption of a hard disk partition***

- ***] to [the Client Administrator]***

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [***On-the-Fly Decryption/Encryption SFP***] to restrict the ability to [***modify***] the security attributes [***the hard disk encrypted partitions***] to [***Client Administrator***].

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [***On-the-Fly Decryption/Encryption SFP***] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [***none***] to specify alternative initial values to override the default values when an object or information is created.

Application Note: Element 3.2 specifies that no one can change the default value for the attributes used to enforce the SFP. When a new partition is added the default will always be restrictive. The Client Administrator can change the attribute for the partition using FMT_MSA.1.

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [***see table below***] the [***see table below***] to [***see table below***].

Table 3 Management of TSF Data in the TOE

Operations	TSF Data	Roles
Remove	Registered user identifier	Client Administrator
Change	Own Password	Registered user
Change	Decrypt the disk	Client Administrator
Change	Encrypt the disk	Client Administrator and registered user
View	Evaluated Configuration Setting from Installation Process -password policy -Client Monitor disabled -Authenti-Check and One-Time Password disabled -Single Sign-On disabled -Token authentication disabled -Autologon disabled -Grace restarts disabled -Disk status (encrypted/decrypted) -Removable Storage access and encryption policies	Client Administrator and Registered user

FMT_SMF.1 *Specification of Management Functions*

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

- ***Initial encryption/terminal decryption***
- ***Audit***]

Application Note: The initial encryption/terminal decryption management function is the mechanism for modifying the SFP on-the-fly decryption/encryption function; therefore, the on-the-fly function is not listed because it is redundant.

FMT_SMR.1 *Security roles*

FMT_SMR.1.1 The TSF shall maintain the roles [***Client Administrator, Policy Administrator, registered user***].

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

Application Note: The Policy Administrator only creates the installation files and has no management functions associated with the TOE following installation.

5.1.1.6 Protection of the TSF (FPT)

FPT_RVM.1(1) *Non-bypassability of the TSP (TOE)*

FPT_RVM.1(1).1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP_TOE_EXP.1 *TSF partial domain separation*

FPT_SEP_TOE_EXP.1The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI

FPT_TST.1 *TSF testing*

FPT_TST.1.1 The TSF shall run a suite of self tests [***during initial start-up***] to demonstrate the correct operation of [***GEFS***].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [***GEFS***].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

5.1.1.7 TOE Access (FTA)

FTA_TAB.1 *Default TOE access banners*

FTA_TAB.1.1 Before establishing a user session, the TSF should display an advisory warning message regarding unauthorized use of the TOE.

5.1.2 TOE SECURITY ASSURANCE REQUIREMENTS

This section lists the assurance requirements the TOE will meet to be evaluated at Evaluation Assurance Level 4. The following components are taken from CC part 3. The components in the following section have no dependencies unless otherwise noted. These components are included by reference only as there are no parameters to be assigned; the body can be found in CC part 3.

ACM_AUT.1	Partial CM Automation
ACM_CAP.4	Generation Support and Acceptance Procedures
ACM_SCP.2	Problem Tracking CM Coverage
ADO_DEL.2	Detection of Modification
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.2	Fully defined external interfaces
ADV_HLD.2	Security enforcing high-level design
ADV_IMP.1	Subset of the implementation of the TSF
ADV_LLD.1	Descriptive low-level design
ADV_RCR.1	Informal correspondence demonstration
ADV_SPM.1	Informal TOE security policy model
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.1	Identification of Security Measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: high-level design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing—sample
AVA_MSU.2	Validation of Analysis
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.2	Independent vulnerability analysis

5.1.3 STRENGTH OF FUNCTION

The overall strength of function requirement is SOF-medium. The strength of function requirement applies to FIA_SOS.1 which constrains the passwords used for the password-based authentication mechanism defined in FIA_UAU.2 and FIA_UAU.2. The SOF claim for this requirement is SOF-medium. The strength of the “secrets” mechanism is consistent with the objectives of authenticating users (O.PARTIAL_TOE_ACCESS). Strength of Function shall be demonstrated for the password-based authentication mechanisms to be SOF-medium, as defined in Part 1 of the CC. Specifically, the local authentication mechanism must demonstrate adequate protection against attackers possessing a moderate attack potential.

5.2 Security Requirements for the IT Environment

The following requirements are taken from CC part 2 except for those explicitly stated, denoted by _EXP in the SFR ID.

Table 4 Functional Components for the IT environment

Item	SFR ID	SFR Title
30.	FAU_SAR.1	Audit review
31.	FAU_STG.1	Protected audit trail storage
32.	FIA_UAU_ENV_EXP.2	User authentication before any action (Client Computer O/S)
33.	FIA_UID_ENV_EXP.2	User identification before any action (Client Computer O/S)
34.	FPT_AMT.1	Abstract machine testing
35.	FPT_RVM.1(2)	Non-bypassability of the TSP (Platform)
36.	FPT_SEP_ENV_EXP.1	TSF Environment partial domain separation
37.	FPT_STM.1	Reliable time stamps

5.2.1.1 Security Audit (FAU)

FAU_SAR.1 Audit review

FAU_SAR.1.1 **Refinement:** The **IT environment** shall provide [***authorised users***] with the capability to read [***all***] from the audit records.

FAU_SAR.1.2 **Refinement:** The **IT environment** shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 **Refinement:** The **IT environment** shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 **Refinement:** The **IT environment** shall be able to [***prevent***] unauthorised modifications to the stored audit records in the audit trail.

5.2.1.2 Identification and Authentication (FIA)

FIA_UAU_ENV_EXP.2 User authentication before any action (Client Computer O/S)

FIA_UAU_ENV_EXP.2.1 The IT Environment shall require each Client Computer user after the initial start-up to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID_ENV_EXP.2. User identification before any action (Client Computer O/S)

FIA_UID_ENV_EXP.2.1 The IT Environment shall require each Client Computer user after the initial start-up to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.2.1.3 Protection of the TSF (FPT)

FPT_AMT.1 Abstract machine testing

FPT_AMT.1.1 **Refinement:** The **IT Environment** shall run a suite of tests [***at the request of an authorised user***] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

FPT_RVM.1(2) Non-bypassability of the TSP (Platform)

FPT_RVM.1(2).1 **Refinement:** The **IT Environment platform** shall ensure that **its functions the TSP relies** are invoked and succeed before each function within **its scope of control** is allowed to proceed.

FPT_SEP_ENV_(EXP).1 TSF Environment partial domain separation

FPT_SEP_ENV_(EXP).1.1 The TSF Environment shall provide hardware that provides virtual memory management and at least two execution rings for executing software (user mode and kernel mode), and an operating system to support these functions.

FPT_SEP_ENV_(EXP).1.2 The TSF Environment shall provide an operating system that provides process separation and access control to files to protect the TOE from interference, tampering and unauthorized access modifications during operation and at rest.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 **Refinement:** The **IT Environment** shall be able to provide reliable time stamps for **the TOE's** use.

6.0 TOE Summary Specification

Table 5 Mapping TOE Security Functions and Requirements

No.	IT Security Function	Security Functional Requirements and the IT Environment Requirements
1.	Security Audit	FAU_GEN.1
		FAU_GEN.2
		(IT Environment) FAU_SAR.1, FAU_STG.1, and FPT_STM.1
2.	Cryptographic Support	FCS_CKM.1
		FCS_CKM.4

No.	IT Security Function	Security Functional Requirements and the IT Environment Requirements
		FCS_COP.1*
3.	Data Protection	FDP_IFC.2
		FDP_IFF.1
4.	Identification and Authentication	FIA_AFL.1
		FIA_SOS.1
		FIA_UAU.2
		FIA_UAU_TOE_EXP.2
		FIA_UID.2
		FIA_UID_TOE_EXP.2
		FIA_UAU.7
		(IT Environment) FIA_UAU_ENV_EXP.2
		(IT Environment) FIA_UID_ENV_EXP.2
		(IT Environment) FPT_STM.1
5.	Security Management	FMT_MSA.1
		FMT_MSA.2
		FMT_MSA.3
		FMT_MOF.1
		FMT_MTD.1
		FMT_SMF.1
		FMT_SMR.1
		(IT Environment) FIA_UAU_ENV_EXP.2
		(IT Environment) FIA_UID_ENV_EXP.2
6.	TOE Protection	FTP_RVM.1(1)
		FPT_SEP_TOE_EXP.1
		FPT_TST.1
		(IT Environment) FPT_AMT.1, FPT_RVM.1(2), FPT_SEP_ENV_EXP.1
7.	Access Banner	FTA_TAB.1

6.1 Security Audit

The GuardianEdge Platform generates records into the Windows system event log file on the client for the security events defined in FAU_GEN.1. Each event record includes: an event identifier, the severity of the (Error, Info, or Warning), and a description of the event indicating the type, source, or policy that generated the event (Internal, Program Action, Initial Setting, Settings Change, or Utility). The Timestamp for each event record is provided by the operating system as part of its systems events files support.

The audit mechanism is automatically started with the start-up of the TOE client, and there is no interface to turn off the audit mechanism.

The following table provides more information on the record contents for each audited security event.

Table 6 Audit Record Information

Security Event.	Severity	Description
Start-up and shutdown of the audit functions		
1001	Info	Internal: Audit functions started. Hard Disk
1	Info	Internal: Audit functions started. Framework
1002	Info	Internal: Audit functions ended. Hard Disk
2	Info	Internal: Audit functions ended. Framework
Successful and Unsuccessful logons		
1003	Info	Program Action: Successful pre-Windows logon/authentication attempted with password. Hard Disk
1005	Info	Program Action: Successful client logon/authentication attempted with password. Hard Disk
1031	Info	Program Action: User logged on after hibernation. Hard Disk
3	Info	Program Action: Successful client logon/authentication attempted with password. Framework
109	Info	Detected logon by user [domain name or local machine name/user name].
1004	Warning	Program Action: Unsuccessful pre-Windows logon/authentication attempted with password. Hard Disk
1006	Warning	Program Action: Unsuccessful client logon/authentication attempted with password. Hard Disk
4	Info	Program Action: Unsuccessful client logon/authentication attempted with password. Framework
110	Info	Detected logoff by user [domain name or local machine name/user name].
Initial encryption and terminal decryption management action		
1027	Warning	Program Action: Partition decryption initiated. Hard Disk
1028	Warning	Program Action: Partition decryption completed. Hard Disk
1029	Info	Program Action: Partition encryption initiated. Hard Disk
1030	Info	Program Action: Partition encryption completed. Hard Disk
All changes to a user’s authentication data		
1017	Info	Program Action: User password changed successfully. Hard Disk
12	Info	Program Action: User password changed successfully. Framework
1018	Info	Program Action: User password changed unsuccessfully. Hard Disk
13	Info	Program Action: User password changed unsuccessfully. Framework
1036	Info	Program Action: User password created. Hard Disk
27	Info	Program Action: User password created. Framework
Maximum number of unsuccessful logon attempts reached; logon delay invoked		
1015	Warning	Program Action: Number of pre-Windows logon attempts exceeded the maximum allowed. Hard Disk
1115	Info	Program Action: Logon delay of sixty seconds instituted.

Security Event.	Severity	Description
11	Warning	Program Action: Number of client logon attempts exceeded the maximum allowed. Framework
1016	Warning	Program Action: Number of client logon attempts exceeded the maximum allowed. Hard Disk
1116	Info	Program Action: Logon delay of sixty seconds lifted.
1117	Info	Program Action: Normal operations resumed: logon delays will be instituted after [*number*] attempts, as per policy.
Registered user added and removed.		
1021	Info	Program Action: Client Administrator has unregistered user. Hard Disk
16	Info	Program Action: Client Administrator has unregistered user. Framework
194	Info	Program Action: Client Administrator [*username*] unregistered user [*username*].
1025	Info	Program Action: User registration completed. Hard Disk
20	Info	Program Action: User registration completed. Framework
Attempts to install/uninstall the product		
1019	Warning	Program Action: User program uninstallation attempted. Hard Disk
14	Warning	Program Action: User program uninstallation attempted. Framework
1032	Info	Program Action: Client program installation attempted. Hard Disk
23	Info	Program Action: Client program installation attempted. Framework
100	Info	The GuardianEdge Removable Storage service was installed.
101	Info	The GuardianEdge Removable Storage service was removed.
102	Info	The GuardianEdge Removable Storage service could not be removed.

The TOE audit security function requires the following support from its IT Environment to provide the audit security service:

- Access control protection of the Windows system event log file from unauthorized access.
- A mechanism for administrators to periodically and, as required, view the audit records in the Windows system log file.
- A timestamp provided to the TOE from its platform.

6.2 Cryptographic Support

FIPS 140-2 Certificate (No. 515): http://csrc.nist.gov/cryptval/140-1/140crt/140crt515.pdf

Covers: AES, SHA-1, HMAC-SHA-1, and RNG.

The FIPS 140-2 library includes:

- A symmetric algorithm, Advanced Encryption Standard (AES) in Cipher Block Chaining mode, with a 256-bit encryption key. The AES implementation is optimized for fast bulk encryption and decryption. The 256-bit key provides industry standard protection against brute-force and dictionary-based attacks.

- A secure hashing algorithm (SHA-1) functionality which computes a condensed representation of a data file, taking in variable-length input and putting out a 160-bit hash value. It is a one-way hashing function, so it is computationally unfeasible to deduce the original file from a given hash value. SHA-1 is a FIPS standard.
- A cryptographic random number generator (RNG) for generating random numbers, the FIPS-186-2 random number generator from FIPS 186-2 appendix 3.1 (with change notice 1 applied).

In addition, the GuardianEdge Platform uses Elliptic Curve Cryptography (ECC) for asymmetric public/private key cryptography. The Elliptic Curve Encryption Scheme (ECES) is the standard IEEE P-1363 implementation. Compliance to this standard is by vendor assertion. A key component of this scheme is the Elliptic Curve Diffie-Hellman (ECDH) algorithm: DL/ECKAS-DH1 (Discrete Log/Elliptic Curve Key Agreement Scheme Diffie-Hellman version 1), using derivation primitive ECSVDP-DH (Elliptic Curve Secret Value Derivation Primitive – Diffie-Hellman version). This algorithm is used with the key derivation function KDF2. ECC was chosen because it gives strong security with keys that are small relative to comparable ciphers, such as RSA.

SHA-1 is used to protect the integrity of the cryptographic library as part of the self-tests. SHA-1 is also used on the WEK and the UPC values to support the authentication process.

Key Destruction: When keys are changed or decommissioned, the areas of disk where the encrypted form was stored are over-written with zeros, or are over-written with the new encrypted key. Key destruction is covered by the FIPS 140-2 certification. For the AES algorithm, the vendor asserts a new WEK replaces an old one when a client is reinstalled using the same caliber of protection as the FIPS 140-2 certified keys.

6.2.1 HARD DISK ENCRYPTION

For hard disk encryption, to support initial encryption and on-the-fly decryption: the media drivers use the TOE’s cryptographic library to perform the AES in Cipher Block Chaining (CBC) mode encryption and decryption for the on-the-fly decryption and initial encryption. This crypto operation is FIPS 140-2 certified. The key is the Workstation Encryption Key (WEK). CBC mode requires an Initialization Vector (IV), which ensures that identical sectors encrypt differently even though the same key is used. Use of an IV helps to thwart cryptanalysis of the raw encrypted disk: without it, it would be easier for an attacker to make inferences about the key based on stereotypes (repetitive patterns). The IV is calculated using a pseudo-random algorithm that is initialized with each sector’s relative sector address.

After successful logon, described below in I&A, the WEK is passed to the driver, which provides for the transparent decryption of each sector as it is needed. On each sector read, the driver decrypts using AES in CBC mode, deriving the IV from the relative sector address using a pseudo-random algorithm.

Supporting user registration and authentication: when a user (both registered users and Client Administrators) registers (see Security Management below), a 32-byte (256-bit) random code is generated using the Random Number Generator algorithm. This unique number is referred to as the User Private Code (UPC) and uniquely identifies each user. The user’s password is used to generate the user’s Elliptic Curve Cryptography (ECC) public and private keys. These ECC keys are in turn used to protect the UPC, and the Workstation Encryption Key (WEK) is encrypted with the UPC. When a user authenticates to GuardianEdge Hard Disk, the user’s private ECC key is used to decrypt the UPC, and from this the WEK is obtained, to perform the encryption and decryption of hard disk data.

6.2.2 REMOVABLE STORAGE ENCRYPTION

For removable encryption, to support initial encryption and on-the-fly decryption/encryption: the media drivers use the TOE's cryptographic library to perform the AES in Cipher Block Chaining (CBC) mode encryption and decryption for the on-the-fly decryption/encryption and initial encryption. This crypto operation is FIPS 140-2 certified. The key is the File Encryption Key (FEK). CBC mode requires an Initialization Vector (IV), which ensures that identical sectors of data encrypt differently even though the same key is used. Use of an IV helps to thwart cryptanalysis of the raw encrypted file: without it, it would be easier for an attacker to make inferences about the key based on stereotypes (repetitive patterns). The IV is calculated using a pseudo-random algorithm that is initialized with the block offset from the head of the encrypted data in the file.

After successful authentication, the FEK is passed to the driver, which provides for the transparent decryption of each sector as it is needed. On each sector read, the driver decrypts using AES in CBC mode, the IV is calculated using a pseudo-random algorithm that is initialized with the block offset from the head of the encrypted data.

Supporting authentication: for removable storage authentication is on a per file basis, successful authentication results in access to the FEK (which is decrypted with the respective authentication key).

The authentication keys for the respective access methods are shown in the following table:

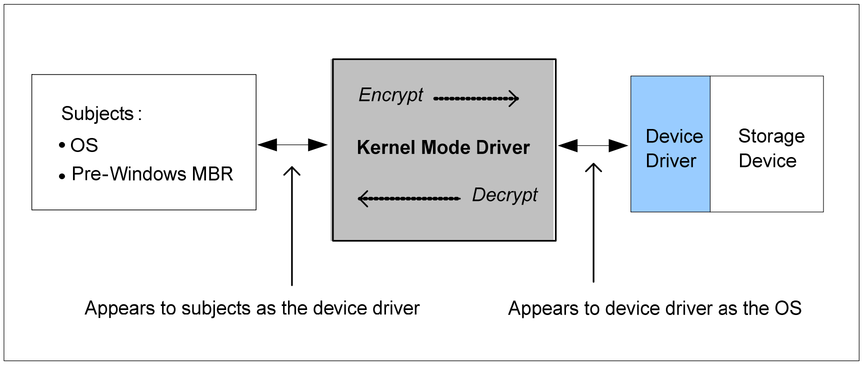
Table 7 Authentication methods, authentication keys and cryptographic operations

Access method	Source of authentication key	Cryptographic operation
Password based	Key derived from user password with KDF2	AES decryption to get FEK

6.3 Data Protection

The data protection security function uses the TOE's FIPS 140-2 certified cryptographic functions (see below) to ensure all data on encrypted partitions on the hard disk and removable storage devices is protected by encryption when not in use (i.e., at rest). All data includes the Windows operating system files, swap files, hibernation files, paging files, executables all data stored on the hard disk, and all unused sectors, as specified in the evaluated configuration. Encrypted data also includes encrypted files on removable storage devices. The GEFS is not encrypted since it is required to bootstrap the system. Encrypted partitions are the partitions on the hard disk and removable storage devices that have been encrypted through the initial encryption process. The initial encryption is performed during installation and as a management function, as specified in FMT_MOF.1.

All data written and read from the encrypted partitions and removable devices passes through the TOE kernel-mode driver, which is the interface for the data protection security function. The protection is applied to all data received or sent to processes that are reading or writing to the encrypted partitions or encrypted files on removable storage devices. The O/S registry was updated during the installation process and initial encryption process to call the TOE driver when data is to be read or written to an encrypted partition. For removable storage devices O/S driver hooks are made for the device after device insertion. The kernel mode driver then calls the device driver of the hard disk or removable storage to provide the interface to the data itself. Then, for hard drive partitions, on each sector read or write, the driver decrypts or encrypts using AES in CBC mode, using an IV derived from the relative sector address. For removable storage devices, on each sector read or write, the driver encrypts using AES in CBC mode, the IV is derived with a pseudo-random number algorithm initialized with the block offset from the head of the encrypted data. The following illustrates the process.



Data Protection Encryption Function

For hard disk encryption, this data protection function does not grant or deny access based on individual users. If a user has access to an application or the operating system on the Client Computer, their access to the data on the media is controlled by the operating system and not the TOE. However, to ensure only registered TOE users have access to the protected data and to prevent by-passing the TOE security functions, as described below in Partial Self-protection, the data protection function is linked to the I&A access control function as follows: after successful logon, the WEK is passed to the TOE hard disk. Therefore, if there are no registered users logged onto the Client Computer there is no key loaded into the driver and therefore no cryptographic operations occur. Data is still passed but users would receive it encrypted.

For removable storage encryption, the data protection function operates at file level, and so relies on the operating system to control access to the encrypted file. Only if the user can both access the encrypted file and provide the correct password or other authentication method, will the user be able to read, or write sectors in the encrypted file. On successful authentication the FEK is passed to the removable storage driver. FEK keys are cached (per user) so that groups of files encrypted with the same password will not repeatedly ask for the password.

6.4 Identification and Authentication

The TOE Identification and Authentication function uses a password-based mechanism to control access to the TOE and its functions at two access points: when accessing the Client Computer during the computer start-up process, and when starting the Client Console application program to access the TOE management function. Both instances of the TOE password mechanism use the same password policy, which is defined by the Policy Administrator during the installation process. Both instances of the password-based mechanism obscures the passwords typed at the logon screen by displaying bullet characters in place of the characters typed.

I&A to control access to the Client Computer:

The pre-Windows identification and authentication mechanism is implemented in the GEFS. The installation process inserts the hooks so this environment takes control from the platform after the BIOS loads but before Windows loads. Users must successfully log on to the TSF for the client start-up process to proceed, enforcing that only registered users get access to the Client Computer when it's started. The user registration function is a Security Management function. The logon process is called during Client Computer start-up and restart.

The following information describes the authentication process using the user-entered parameters name and password:

- Validate the account credentials using name compared to the name of each user record stored in GEFS.
- If the account exists, then generate ECC public/private keys using name and password as the seed.
- Compare the user's ECC public key with the ECC public key stored in GEFS.
- If they match, then decrypt the UPC using the ECC private key; otherwise, abort the authentication process.
- Validate the UPC by calculating the SHA-1 of the UPC and comparing it with the SHA-1 value stored in GEFS.

Once the Client Computer is started, access to the computer and its protected data is controlled by the Client Computer platform operating system.

I&A to control access to the Client Console application program:

Activated when a user selects the GuardianEdge application program from the operating system, the I&A mechanism controlling access to the Client Console interface is the same as the Client Computer I&A mechanism, as described above.

Password Policy:

The password policy is defined by the Policy Administrator during the installation process. The User and Administrator guidance documents provide the specific parameters used in the evaluated configuration to ensure the password mechanism meets the SOF-medium requirements. These parameters are not published in the ST to minimize the information provided to potential threat agents.

When the management function to change a password is activated, this password complexity mechanism is used to check passwords before they are accepted. The configuration parameters for these are defined in Section 5, the default, 0, disables the constraint.

Note: When accented characters are used to satisfy the uppercase and lowercase requirements these characters are not displayed on the password screens.

The TOE authentication failure handling mechanism stops the authentication process for 1 minute when the policy-administrator-defined threshold of failed passwords is reached. The logon screen displays notice of the delay and provides a countdown. The Client Computer platform provides the clocking for measurement of the 1 minute delay.

I&A to control access to the Encrypted Files on Removable Storage Devices

When a removable device is connected to the computer driver hooks are added to the O/S. Authentication for files is per file, though groups of files maybe encrypted using the same credentials. The TOE automatically caches (per user) and suppresses authentication prompts for files encrypted with authentication information the user provided previously during the session. Users must successfully provide the correct authentication information in order to read or write to a file. As the encrypted file is also managed by the O/S the user needs appropriate file system ACLs to be able to operate on the encrypted file.

The following describes the authentication process used during access to an encrypted file on a removable storage device:

- Validate the cached authentication information associated with the user.
- If the authentication information is not present request it from the user.
- For password based access, the authentication information is the user's password. The password is used to derive an access key with KDF2.
- The access key is used to decrypt the FEK from a field in the encrypted file header.
- KDF2 is used to derive a decryption key from the user password, the decryption key is used to decrypt the FEK. A SHA-1 hash of the FEK is stored. In order to verify that the correct password was used, the decrypted FEK is hashed with SHA-1 and the hash is compared to the stored FEK hash.

Once this access process is complete the FEK is passed to the Removable Storage driver.

6.5 Security Management

The security management function is performed primarily through the Client Console interface. All management functions except adding a registered user are performed through the Client Console interface.

Adding a registered user is a self-registration process done through the "I&A to control access" to the Client Computer interface, used in Section 6.4. When a user logs onto the operating system after the Client Computer start-up process, if the user name authenticated by the O/S logon process does not exist as a registered user of the TOE, the TSF will present the I&A to control access to the Client Computer interface with an option to register or bypass the registration process. When a users registers, by setting their password, they are established as a registered user.

The Client Console interface provides Client Administrators the ability to remove registered users and perform initial encryption or terminal decryption on selected partitions. Client Administrators can also view certain configuration settings (defined in the installation process) through the console interface. The complete configuration settings are available in protected LOG files, allowing the Client Administrator to verify the evaluated configuration. Registered users are able to change their own password using the Client Console.

The following policy and configuration parameters are set by the Policy Administrator during the installation process:

- Availability of Single Sign-On feature,
- The number of failed authentication attempts before the delay,
- The complexity requirements for the passwords,
- Whether a Registration password is required before a user can register,
- How many users are allowed to register,

- Authentication method,
- Message displayed to notify the user that they need to register,
- Number of grace restarts,
- Availability of automated and semi-automated password recovery methods,
- Message displayed to users having difficulty authenticating,
- Whether the client will report data at designated intervals to central server,
- AES encryption strength,
- Access banner,
- Whether to prefill the logon with the most recent user name and/or domain,
- Which partitions to encrypt and when,
- Whether to encrypt all sectors on the disk, even if they are unused,
- Whether to enable power loss protection during initial encryption,
- Who is allowed to perform terminal decryption of the disk (Client Administrators and/or users),
- The location of GEFS,
- Whether or not to enforce communication with the central server,
- Access policy for removable media (read, read/write, none),
- Encryption policy for removable media (all files, new files, none),
- Whether to copy the Access Utility to removable media or not,
- Encryption method (password and/or certificate),
- Whether or not to encrypt with a master certificate, and if so, which,
- Whether or not to encrypt with a group key, and, if so, which,
- Whether or not to allow users to encrypt files in a self-extracting executable format, and
- Defining the Client Administrators.

To access the GuardianEdge Client Console application, users select the application program from the Windows operating system and then must authenticate to the console application with their password. Once authenticated registered users are presented with an interface that only lets them change their password, Client Administrators are provided an interface to perform the other functions.

The management functions for the on-the-fly decryption/encryption and initial encryption are linked. By performing initial encryption on a partition the Client Administrator is also enabling on-the-fly decryption/encryption for that partition. Similarly, by performing terminal decryption on a partition they are effectively disabling on-the-fly decryption/encryption for that partition. If a new disk partition is added to the Client Computer, the Client Administrator must perform initial encryption on that partition for the on-the-fly decryption/encryption to apply to the partition.

6.6 TOE Protection

The TOE uses a combination of architecture and security mechanisms to work in concert with its platform to ensure the TSF cannot be bypassed, corrupted, or otherwise compromised. In general, the TSF architecture uses a combination of:

- A set of well-defined subsystems, with well-defined interfaces, that utilize protections provided by the IT Environment platform.
- A processing sequence to protect itself from being bypassed, interfered with, or tampering.
- A set of self-tests run during start-up.

The TOE's TSF architecture includes subsystems that run either in the pre-Windows environment, as kernel mode processes, or as user application processes. These are simple computing components that are single-threaded, managing one process at a time, take the input from their interface, process it, and pass it to the next interface.

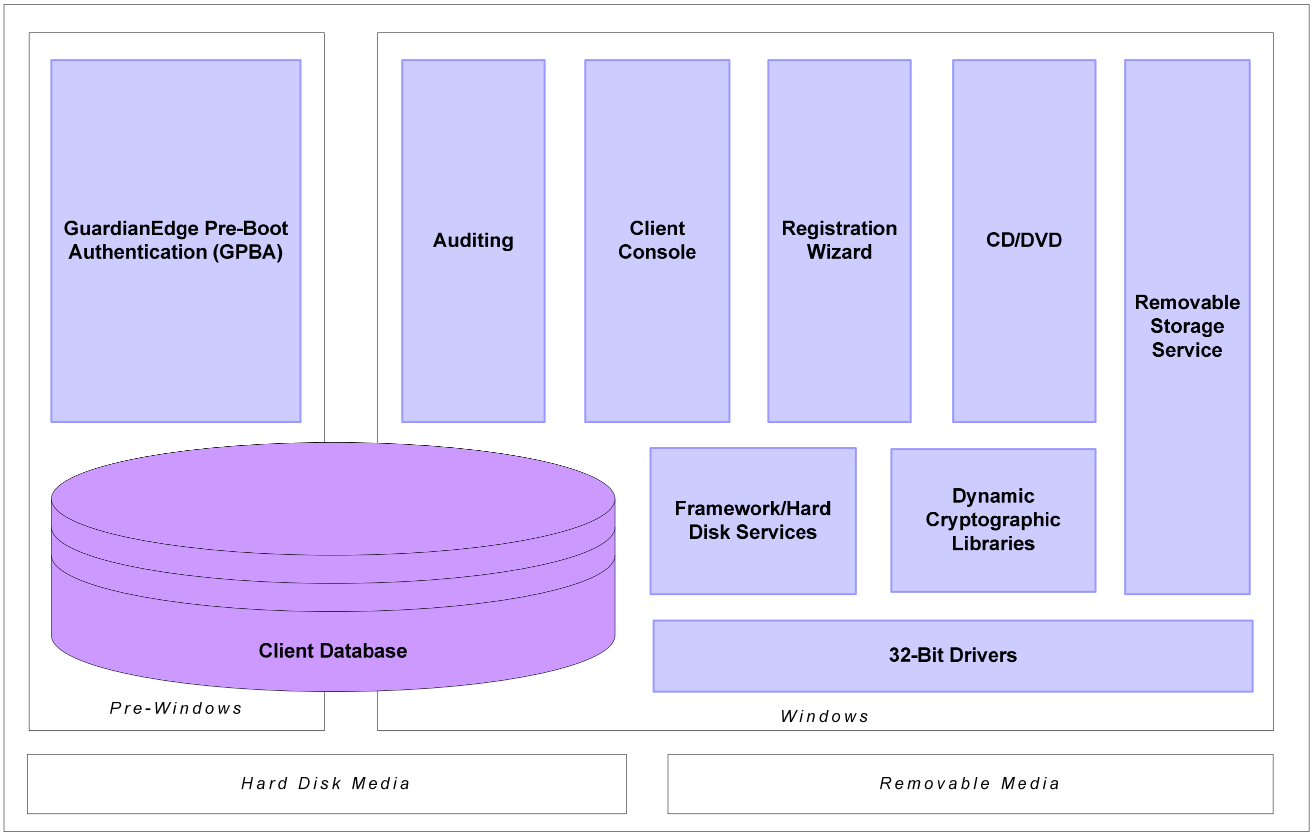
The TSF depends on the IT environment to provide:

- Host platform (processor and O/S) prevents unauthorized access to TOE data and stored executables, i.e., that the TOE is only accessible through its specified interfaces.
- Host platform (processor and O/S) provides separate address space and execution process for the TOE distinct from other applications.

Well-Defined Subsystems

Note: the design documentation provided to meet the EAL4 augmented with ALC_FLR.3 assurance provides details on these subsystems and their interfaces.

The following diagram illustrates the subsystems of the TSF architecture. Note, these subsystems are the same as the components identified in Section 2, TOE description.


GuardianEdge Pre-Boot Authentication (GPBA)
Auditing
Client Console
Registration Wizard
CD/DVD
Removable Storage Service
Framework/Hard Disk Services
Dynamic Cryptographic Libraries
Client Database
32-Bit Drivers
Pre-Windows
Windows
Hard Disk Media
Removable Media

Client Computer

TOE Subsystems

The following table identifies the subsystems of the Client Computer and their processing environments.

Table 8 Subsystems and Processing Environments

TSF Subsystem	Processing Environment	Notes on Self-Protection
GPBA	Pre-Windows processes and files	Protected by the 'Processing Sequence' defined below. If it's bypassed or modified the result will be no access to the storage resources.
Client Database	Pre-Windows and Windows process	Protected by the processing sequence, if it's bypassed or modified the result will be no access to the storage resources.
32-Bit Drivers	Kernel mode processes	Relies on the IT Environment hardware platform kernel execution rings and its supporting operating system.
Auditing	User application processes	Relies on the hardware user process execution rings and O/S process separation, ensuring the TOE is only accessible through its specified interfaces.

TSF Subsystem	Processing Environment	Notes on Self-Protection
Client Console	User application processes	Relies on the hardware user process execution rings and O/S process separation, ensuring the TOE is only accessible through its specified interfaces.
Registration Wizard	User application processes	Relies on the hardware user process execution rings and O/S process separation, ensuring the TOE is only accessible through its specified interfaces.
CD/DVD	User application processes	Relies on the hardware user process execution rings and O/S process separation, ensuring the TOE is only accessible through its specified interfaces.
Removable Storage Service	User application processes	Relies on the hardware user process execution rings and O/S process separation, ensuring the TOE is only accessible through its specified interfaces.
Framework/Hard Disk Services	User application processes	Relies on the hardware user process execution rings and O/S process separation, ensuring the TOE is only accessible through its specified interfaces.
Dynamic Cryptographic Libraries	User application processes	Relies on the hardware user process execution rings and O/S process separation, ensuring the TOE is only accessible through its specified interfaces.

The pre-Windows subsystem functions are described in the “processing sequence” section below. The 32-bit Drivers subsystem ensures that data destined for its media is encrypted before being stored on the media, and decrypted when it leaves its media in the other direction. The Auditing, Client console, Registration Wizard, CD/DVD, Removable Storage Service, Framework/Hard Disk Services, and Dynamic Cryptographic Libraries subsystems run as user processes and include simple GUI consoles/prompts/dialogs and the FIPS 140-2 cryptographic libraries.

Well-defined interfaces - The design documentation provided to meet the EAL4 augmented with ALC_FLR.3 assurance provides details on the user and IT environment interfaces where the non-bypassability is enforced.

The TOE provides additional protection for the interface to management sessions as defined by O.MANAGE. The TOE management is provided by a software application component with a GUI user interface. This functions as a standard windows application with its single external interface that is local, one-user-of-the-interface-at-a-time, GUI external interface. Access to the Client Console interface is controlled by the TSF I&A mechanism, described in Section 6.4. Only the user can successfully authenticate to the User Client console and only the Client Administrator can access the Administrator Client console.

The Processing Sequence for Hard Disk Encryption

The aspects of the general processing sequence that provides self-protection are as follows:

- During installation the platform MBR is copied to another location and replaced by the GMBR.
- The GMBR directs the processing to the GPBA, which executes a self-test function that verifies the integrity of the pre-Windows code and data and runs the FIPS 140-2 crypto library set of self tests.
- Upon successful self-test the GPBA executes the I&A function.
- Upon successful authentication a user key is generated by the crypto library and used to load the workstation encryption key and control is passed back to the original MBR.
- The original MBR starts Windows XP, via Intel CPU driver using the GEHD device driver function (loaded with the workstation key from the authentication process) to decrypt the Window XP code from the hard disk.

This provides protection by the following:

- If someone tries to bypass the I&A function they will not have generated the cryptographic user key that loads the workstation encryption key. So, even if e.g., they can load another operating system via a floppy, the protected media will remain encrypted.
- The integrity checks on the pre-Windows code identify tampering and stop the access sequence.
- If someone should tamper with the self-test code and other pre-Windows code and present a false positive to the integrity check, the tampered (rogue) code will not be able to create the cryptographic based user keys required to load the workstation key, as described above.

The Processing Sequence for Removable Storage

The sequence and protections for Hard disk encryption apply first, and in addition the following Removable Storage procedures apply, once Windows is loaded and the user starts to work with an encrypted file stored on a Removable Storage device.

Aspects of the general processing sequence that provides self-protection are as follows:

- Authentication is per file, and upon successful authentication to gain access to a file, a user key is generated by the crypto library and used to load the file encryption key (FEK) and the FEK is passed to the Removable Storage driver.

This provides protection by the following:

- If someone tries to bypass the Removable Storage I&A function for a given file, they will not have generated the cryptographic user key that loads the file encryption key. So, even if they put the Removable Storage Device in a computer with the intent of by passing the I&A, the protected file will remain encrypted.
- If someone should tamper with the self-test code of removable storage code and present a false positive to the integrity check, the tampered (rogue) code will not be able to create the cryptographic based user keys required to load the file key, as described above.

Self-Tests

The TOE implements a suite of self-tests invoked at startup to verify the integrity of the Client Database and perform the operational checks on the cryptographic library as required in the FIPS 140-2 certification.

The self-tests are implemented using the standard test vectors as published in the associated standard where available. In some cases, a subset of the full set of test vectors from the associated standard (where applicable) is implemented to reduce time and space overheads of the test suite. This function is implemented at the start-up of the Client Computer.

The TOE verifies checksums on the cryptographic module. The TSF implements checksums and secure hash on TSF data meeting the requirement. More specifically, the TOE verifies cryptographic checksums on its Linux (Pre-Windows) executables, drivers, and libraries at startup to resist software tampering.

The function is implemented by restarting the TSF and integrity errors are reported during the process.

6.7 Access Banner

The TOE displays a GuardianEdge Hard Disk Encryption access banner (advisory warning message) as part of its logon screen. The advisory message is defined by the Policy Administrator during the installation process and is displayed at start-up.

6.8 SOF Claims

The threat level for the TOE authentication function is assumed to be SOF-medium. This defines a level of authentication strength of function where analysis shows that the function provides basic protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

The password-based mechanism in the Identification and Authentication function, Section 6.4, is realized by probabilistic or permutational mechanisms. The methods used to provide difficult-to-guess passwords are probabilistic. The specific password policy is specified in the FIA_SOS.1 as providing the following constraining factors:

- Minimum of eight total characters,
- At least one non-alphanumeric character;
- At least one UPPERCASE letter (A-Z and 32 accented uppercase characters); and
- At least one digit (0-9).]

The SOF claim for Identification and Authentication is SOF-medium.

6.9 TOE Assurance Measures

The following table identifies the TOE Assurance Measure that meets the EAL4 augmented with ALC_FLR.3 assurance requirements. Following the table each TOE Assurance Measure is listed with a short description of how it satisfies the assurance requirements.

Table 9 Mapping of Assurance Requirements to Assurance Measures

Security Assurance Requirement Component	TOE Assurance Measure Identifier	How Satisfied and Rationale
ACM_AUT.1.1D ACM_AUT.1.2D ACM_AUT.1.1C ACM_AUT.1.2C ACM_AUT.1.3C ACM_AUT.1.4C	AM.CM_DOC	GuardianEdge configuration management documentation. Describes the automated tools that support controlled changes to the implementation representation.
ACM_CAP.4.1D ACM_CAP.4.2D ACM_CAP.4.3D ACM_CAP.4.1C ACM_CAP.4.2C ACM_CAP.4.3C ACM_CAP.4.4C ACM_CAP.4.5C ACM_CAP.4.6C ACM_CAP.4.7C ACM_CAP.4.8C ACM_CAP.4.9C ACM_CAP.4.10C ACM_CAP.4.11C ACM_CAP.4.12C ACM_CAP.4.13C	AM.CM_DOC	GuardianEdge configuration management documentation. Describes the system to clearly identify the TOE and its associated configuration items and the system to properly control changes to them.
ACM_CAP.4.1E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
ACM_SCP.2.1D ACM_SCP.2.1C	AM.CM_DOC	The GuardianEdge Platform configuration item list. Provides documentation that configuration management includes the TOE implementation representation, design, tests, user and administrator guidance, the CM documentation and security flaws
ACM_SCP.2.1E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
ADO_DEL.2.1D ADO_DEL.2.2D ADO_DEL.2.1C ADO_DEL.2.2C ADO_DEL.2.3C	AM.ADO_DEL	The GuardianEdge Platform delivery documentation. Provides documentation that describes all procedures used to maintain security and detect modifications or substitution of the TOE when distributing it to the user's site.
ADO_DEL.2.1E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.

Security Assurance Requirement Component	TOE Assurance Measure Identifier	How Satisfied and Rationale
ADO_IGS.1.1D ADO_IGS.1.1C	AM.USR_DOC	The GuardianEdge Platform secure installation, generation, and start-up procedures. Provides documentation that describes the procedures and steps for the secure installation, generation, and start-up of the TOE in its evaluated configuration.
ADO_IGS.1.1E ADO_IGS.1.2E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
ADO_IGS.1.2E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
ADV_FSP.2.1D ADV_FSP.2.1C ADV_FSP.2.2C ADV_FSP.2.3C ADV_FSP.2.4C ADV_FSP.2.5C	AM.ADV_FSP	The GuardianEdge Platform functional specification. Provides documentation that describes how the security functions of the TOE meet the functional requirements specified in the ST.
ADV_FSP.2.1E ADV_FSP.2.2E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
ADV_HLD.2.1D ADV_HLD.2.1C ADV_HLD.2.2C ADV_HLD.2.3C ADV_HLD.2.4C ADV_HLD.2.5C ADV_HLD.2.6C ADV_HLD.2.7C ADV_HLD.2.8C ADV_HLD.2.9C	AM.DES_DOC	The GuardianEdge Platform high-level design. Provides documentation that describes the TSF in terms of major structural units, its interfaces and a correct realization of the functional specification.
ADV_HLD.2.1E ADV_HLD.2.2E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
ADV_IMP.1.1D ADV_IMP.1.1C ADV_IMP.1.2C	AM.ADV_IMP	A subset of the implementation representation for the GuardianEdge Platform. Provides documentation that the implementation representation is sufficient to satisfy the functional requirements of the ST and is a correct realization of the low-level design.
ADV_IMP.1.1E ADV_IMP.1.2E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.

Security Assurance Requirement Component	TOE Assurance Measure Identifier	How Satisfied and Rationale
ADV_LLD.1.1D ADV_LLD.1.1C ADV_LLD.1.2C ADV_LLD.1.3C ADV_LLD.1.4C ADV_LLD.1.5C ADV_LLD.1.6C ADV_LLD.1.7C ADV_LLD.1.8C ADV_LLD.1.9C ADV_LLD.1.10C	AM.DES_DOC	The GuardianEdge Platform low-level design. Provides documentation that the low-level design is sufficient to satisfy the functional requirements of the ST and is a correct and effective refinement of the high-level design.
ADV_LLD.1.1E ADV_LLD.1.2E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
ADV_RCR.1.1D ADV_RCR.1.1C	AM.ADV_RCR	The GuardianEdge Platform correspondence analysis documentation. Provides analysis that the ST requirements are completely and correctly implemented throughout the set of design documentation.
ADV_RCR.1.1E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
ADV_SPM.1.1D ADV_SPM.1.2D ADV_SPM.1.1C ADV_SPM.1.2C ADV_SPM.1.3C ADV_SPM.1.4C	AM.ADV_SPM	The GuardianEdge Platform TOE security policy model. Documents the security policy model that describes the rules and characteristics of the security policies and its correspondence with the functional specification. The Security Policy Model requirement for ADV_SPM.1 is met by this Security Target.
ADV_SPM.1.1E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
AGD_ADM.1.1D AGD_ADM.1.1C AGD_ADM.1.2C AGD_ADM.1.3C AGD_ADM.1.4C AGD_ADM.1.5C AGD_ADM.1.6C AGD_ADM.1.7C AGD_ADM.1.8C	AM.USR_DOC	The GuardianEdge Client Administrator guidance. Provides documentation for the administrator on how to administer the TOE in a secure manner.
AGD_ADM.1.1E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.

Security Assurance Requirement Component	TOE Assurance Measure Identifier	How Satisfied and Rationale
AGD_USR.1.1D AGD_USR.1.1C AGD_USR.1.2C AGD_USR.1.3C AGD_USR.1.4C AGD_USR.1.5C AGD_USR.1.6C	AM.USR_DOC	The GuardianEdge Platform user guidance. Provides documentation for secure use of the TOE by its users.
AGD_USR.1.1E	Evaluation.	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
ALC_DVS.1.1D ALC_DVS.1.1C ALC_DVS.1.2C	AM.DES_DOC	The GuardianEdge Platform development security documentation. Provides documentation that the developer's security controls on the development environment are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure that secure operation of the TOE is not compromised.
ALC_DVS.1.1E ALC_DVS.1.2E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
ALC_LCD.1.1D ALC_LCD.1.2D ALC_LCD.1.1C ALC_LCD.1.2C	AM.DES_DOC	The GuardianEdge Platform life-cycle definition documentation. Provides documentation that the developer used a model of the TOE life-cycle.
ALC_LCD.1.1E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
ALC_TAT.1.1D ALC_TAT.1.2D ALC_TAT.1.1C ALC_TAT.1.2C ALC_TAT.1.3C	AM.DES_DOC	The GuardianEdge Platform development tool documentation. Provides documentation that the developer has used well-defined development tools that yield consistent and predictable results.
ALC_TAT.1.1E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
ALC_FLR.3.1C	AM.FLR_DOC	The GuardianEdge flaw remediation procedures.
ALC_FLR.3.2C		
ALC_FLR.3.3C		
ALC_FLR.3.4C		
ALC_FLR.3.5C		
ALC_FLR.3.6C		
ALC_FLR.3.7C		
ALC_FLR.3.8C		
ALC_FLR.3.9C		

Security Assurance Requirement Component	TOE Assurance Measure Identifier	How Satisfied and Rationale
ALC_FLR.3.10C		
ALC_FLR.3.11C		
ALC_FLR.3.1E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
ATE_COV.2.1D ATE_COV.2.1C ATE_COV.2.2C	AM.TST_DOC	The GuardianEdge Platform test coverage analysis. Provides documentation that the testing is sufficient to establish that the TSF has been systematically tested against the functional specification.
ATE_COV.2.1E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
ATE_DPT.1.1D ATE_DPT.1.1C	AM.TST_DOC	The GuardianEdge Platform depth of testing analysis. Provides documentation that the developer has tested the TSF against its high-level design.
ATE_DPT.1.1E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
ATE_FUN.1.1D ATE_FUN.1.2D ATE_FUN.1.1C ATE_FUN.1.2C ATE_FUN.1.3C ATE_FUN.1.4C ATE_FUN.1.5C	AM.TST_DOC	The GuardianEdge Platform test documentation and test procedures. Provides documentation that the developer’s functional tests are sufficient to demonstrate that security functions perform as specified.
ATE_FUN.1.1E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
ATE_IND.2.1D ATE_IND.2.1C ATE_IND.2.2C	AM.ATE_IND	Independent testing and documentation was done by the evaluation team and analysis captured in the ETR Part 2.
ATE_IND.2.1E ATE_IND.2.2E ATE_IND.2.3E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
AVA_MSU.2.1D AVA_MSU.2.2D AVA_MSU.2.1C AVA_MSU.2.2C AVA_MSU.2.3C AVA_MSU.2.4C AVA_MSU.2.5C	AM.AVA_MSU	The GuardianEdge Platform misuse analysis of the guidance. Provides documentation that the guidance is not misleading, unreasonable or conflicting, and includes procedures for all modes of operation, and facilitates prevention and detection of insecure TOE states.

Security Assurance Requirement Component	TOE Assurance Measure Identifier	How Satisfied and Rationale
AVA_MSU.2.1E AVA_MSU.2.2E AVA_MSU.2.3E AVA_MSU.2.4E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
AVA_SOF.1.1D AVA_SOF.1.1C AVA_SOF.1.2C	AM.AVA_SOF	The GuardianEdge Platform strength of TOE security functions analysis. Provides documentation on all probabilistic or permutational mechanisms to show how they meet the ST SOF claims.
AVA_SOF.1.1E AVA_SOF.1.2E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.
AVA_VLA.2.1D AVA_VLA.2.2D AVA_VLA.2.1C AVA_VLA.2.2C	AM.AVA_VLA	The GuardianEdge Platform vulnerability analysis. Provides documentation to determine whether the TOE, in its intended environment, has vulnerabilities exploitable by attackers possessing low attack potential.
AVA_VLA.2.1E AVA_VLA.2.2E AVA_VLA.2.3E AVA_VLA.2.4E AVA_VLA.2.5E	Evaluation	Evaluated by the evaluation team and analysis captured in the ETR Part 2.

7.0 Protection Profile Claims

See Section 1.1 “Identification” on page 5 for statement of PP non-conformance.

8.0 Rationale

8.1 Security Objectives Rationale

8.1.1 SECURITY OBJECTIVES RATIONALE FOR THREATS

The following table verifies all identified security threats are countered by Security Objectives for the TOE and IT-environment. There are no Organizational Policies defined for this ST.

Table 10 Threats, Objectives, and Rationale

Security Threats/OSP	Security Objective	Comments on rationale for tracing and coverage
T.IMPROPER_NOTICE: A user may not receive proper sanctions from inappropriate use because notice of restricted use or other binding conditions was not provided resulting in decreased effectiveness of administrative controls for protecting assets.	O.DISPLAY_BANNER: The TOE will display an advisory warning regarding use of the TOE.	**O.DISPLAY_BANNER** mitigates this risk by ensuring that the TOE displays a banner, configured at installation, that provides all interactive users with a warning about the unauthorized use of the TOE. E.g., to meet policy: Reference: DODI 8500.2 Enclosure 4, Attachment 4 ECWM-1 and ECAN-1
T.MASQUERADE: A malicious user or external IT entity may masquerade as another entity in order to gain unauthorized access to the Client Computer media assets	**O.PARTIAL_TOE_ACCESS:** The TOE will provide mechanisms that control user's logical access to the TOE Client Console and to the TOE mechanism that allows the Client Computer to start-up and make protected data available to the Client Computer users.	**O.PARTIAL_TOE_ACCESS** mitigates this threat by controlling the logical access to the TOE Client Console interface and to the TOE mechanism that allows the Client Computer to start-up and make protected data available. By constraining how authorized users can access these TOE interfaces and by mandating the complexity of the passwords used to authenticate users this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, unauthorized access is further prevented by providing an authentication failure mechanism that delays the logon process after a number of failed login attempts.
	OE.TOE_ENVIR_ACCESS: The IT environment will provide the capability to control users' logical access to the Client Computer after its startup.	**OE.TOE_ENVIR_ACCESS:** provides an identification and authentication mechanism to control users' logical access to the Client Computer for users accessing the TOE after the startup of the Client Computer, which is covered by O.PARTIAL_TOE_ACCESS has controlled the initial access that allows the computer to start-up.

Security Threats/OSP	Security Objective	Comments on rationale for tracing and coverage
	OE.TIMESTAMP: The TOE computing platform will provide reliable time.	**OE.TIMESTAMP** provides a reliable clock to measure the one minute delay for the authentication failure mechanism in O.PARTIAL_TOE_ACCESS.
T.TSF_COMPROMISE: A user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).	O.CORRECT_ TSF_OPERATION: The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.	**O.CORRECT_ TSF_OPERATION** mitigates the T.TSF_COMPROMISE threat by always running a set of tests to ensure proper operations and of critical cryptographic operations and to perform integrity checks on the portions of the TSF that are not encrypted on the hard disk (i.e., protected by the TOE security services).
	O.MANAGE: The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	**O.MANAGE** mitigates this attack by controlling who is able to view and modify security has access to perform security functions and view and change security data and attributes.
	O.PARTIAL_SELF_PROTECTION: The TSF will maintain a domain for its own execution, and implement an architecture and mechanisms that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.	**O.PARTIAL_SELF_PROTECTION** mitigates this threat through its architecture of processes running in protected execution space, well-defined interfaces, and cryptographic controls to prevent bypassing the TSF interfaces.
	OE.PARTIAL_TOE_PROT: The TSF Environment shall provide virtual memory management, execution rings for executing user software and kernel processes to protect the TOE processes from interference and tampering, and file protection to prevent unauthorized access and modifications to TOE.	**OE.PARTIAL_TOE_PROT** mitigates this threat by providing separate execution rings for the TOE user and kernel processes, and by providing operating system file protection for the files comprising the TOE to prevent unauthorized access.

Security Threats/OSP	Security Objective	Comments on rationale for tracing and coverage
	OE.TOE_ENVIR_ACCESS: The IT environment will provide the capability to control users’ logical access to the Client Computer after its startup.	**OE.TOE_ENVIR_ACCESS** mitigates this threat by supporting O.MANAGE by providing the logon function to Client Computer after its startup and the user identifier to facilitate the user self-registration process.
T.UNAUTHORIZED_MEDIA_ ACCESS: An unauthorized user with physical access to the Client Computer may access assets stored on the hard disk and removable storage devices encrypted partitions by subverting the normal computer start-up processes or by removing the media from the computer.	O.MEDIASEC: The TSF must be able to protect the Client Computer media assets on the Client Administrator-specified hard disk partitions and removable storage devices, using encryption.	**O.MEDIASEC** mitigates this threat by providing the authorized Client Administrators the mechanism to perform initial encryption (and decryption on a disk or removable media partition to protect the data at rest and define that partition as a subject for the TOE On-the-Fly Decryption/Encryption SFP.
	O.TRANSPARENT_ENFORCED_ACCESS: The TSF must be able to provide authorized users and system processes read and write access to the Client Computer encrypted partitions in a manner that is transparent to users to ensure the mechanism is always invoked and the data is available to the system, authorized users, and applications and is encrypted when not in use and stored on the encrypted partitions.	**O.TRANSPARENT_ENFORCED_ ACCESS** mitigates this risk by providing the On-the-Fly Decryption/Encryption SFP that ensures all data read from an “encrypted” partition is decrypted and accessible to users and processes, and all data written to an “encrypted” partition” is encrypted to ensure protection when the data is at rest.
T.UNIDENTIFIED_ACTIONS: The administrator may not have the ability to notice potential security violations, thus limiting the administrator’s ability to identify and take action against a possible security breach and hold persons accountable for their actions.	O.AUDIT_GENERATION: The TOE will provide the capability to detect and create records of security relevant events associated with users.	**O.AUDIT_GENERATION** helps to mitigate this threat by recording actions for later review.
	OE.AUDIT_SUPPORT: The IT environment will provide the capability to view audit information, and will protect the stored audit records from unauthorized modification and deletion, and will provide a timestamp for the audit records.	**OE.AUDIT_SUPPORT** helps mitigate this threat by providing the file structure and a timestamp for the audit records and protect access to that file. It also provides a means to view these records.

Security Threats/OSP	Security Objective	Comments on rationale for tracing and coverage
	OE.TIMESTAMP: The TOE computing platform will provide reliable time.	**OE.TIMESTAMP** helps mitigate this threat by providing reliable time for the audit record timestamps.

8.1.2 ASSUMPTIONS ADDRESSED

The table below shows that each identified assumption is countered by at least one security objective for non-IT environment objective. (Objectives for the IT environment correspond to requirements).

Table 11 Mapping of Assumptions to Objectives

Security Assumptions	Security Objective	Rationale for tracing and coverage
A.NET_ACC: It is assumed if the Client Computer is connected to a network, then remote users are required to log on to the Windows operating system to gain access, and that file sharing and other network services that don't require Windows logon and provide remote access to data stored on the Client Computer media are either disabled or there are appropriate network authentication and confidentiality services.	ON.NET_ACC: The environment procedures will ensure that the operational environment is suitable for the threats the TOE is designed to meet. For example, if the Client Computer is connected to a network, then remote users are required to log on to the Windows operating system to gain access, and that file sharing and other network services that don't require Windows logon and provide remote access to data stored on the Client Computer media are either disabled or there are appropriate network authentication and confidentiality services.	A restatement of the assumption and therefore is suitable for covering the assumption.
A.NO_EVIL: It is assumed that administrators are non-hostile, appropriately trained and follow all administrator guidance.	ON.NO_EVIL: The environment procedures will ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.	A restatement of the assumption and therefore is suitable for covering the assumption.
A.NO_MALWARE: It is assumed the operating environment for the TOE runs only software, firmware, or hardware that has been approved by the security officer.	ON.NO_MALWARE: The environment procedures will ensure that the operating environment for the TOE runs only software, firmware, or hardware that has been approved by the security officer.	A restatement of the assumption and therefore is suitable for covering the assumption.
A.NO_UAT: It is assumed that users do not leave the GuardianEdge Client Computer unattended when they are logged on.	ON.NO_UAT: The environment procedures will ensure that users do not leave the GuardianEdge Client Computer unattended when they are logged on.	A restatement of the assumption and therefore is suitable for covering the assumption.
A.USERS: It is assumed that users will protect their authentication data.	ON.USERS: The environment procedures will ensure that users will protect their authentication data.	A restatement of the assumption and therefore is suitable for covering the assumption.

Security Assumptions	Security Objective	Rationale for tracing and coverage
A.NO_LOCAL_ADMIN It is assumed that the user is not defined as a local administrator and has not been given local administrative privileges.	ON.NO_LOCAL_ADMIN The environment procedures will ensure that the user is not defined as a local administrator and has not been given local administrative privileges.	A restatement of the assumption and therefore is suitable for covering the assumption.

8.1.3 ALL OBJECTIVES COVERED

The table below shows the objectives for the TOE and environment and their mapping to the Threats and Assumptions.

Table 12 Reverse Mapping of Security Objectives to Threats/Assumptions

Objective	Threat/OSP
O.AUDIT_GENERATION	T.UNIDENTIFIED_ACTIONS
O.CORRECT_ TSF_OPERATION	T.TSF_COMPROMISE
O.DISPLAY_BANNER	T.IMPROPER_NOTICE
O.MANAGE	T.TSF_COMPROMISE
O.MEDIASEC	T.UNAUTHORIZED_MEDIA_ACCESS
O.PARTIAL_SELF_PROTECTION	T.TSF_COMPROMISE
O.PARTIAL_TOE_ACCESS	T.MASQUERADE
	T.TSF_COMPROMISE
O.TRANSPARENT_ENFORCED_ACCESS	T.UNAUTHORIZED_MEDIA_ACCESS
OE.AUDIT_SUPPORT	T.UNIDENTIFIED_ACTIONS
OE.PARTIAL_TOE_PROT	T.TSF_COMPROMISE
OE.TIMESTAMP	T.MASQUERADE
	T.UNIDENTIFIED_ACTIONS
OE.TOE_ENVIR_ACCESS	T.MASQUERADE
ON.NET_ACC	A.NET_ACC
ON.NO_EVIL	A.NO_EVIL
ON.NO_MALWARE	A.NO_MALWARE
ON.NO_UAT	A.NO_UAT
ON.USERS	A.USERS
ON.NO_LOCAL_ADMIN	A.NO_LOCAL_ADMIN

8.2 Security Requirements Rationale

The rationale for Security Functional Requirements (SFRs) with tracing to security objectives is given in the following table.

Table 13 Mapping of Security Objectives to Security Functional Requirements

Security Objective	Security Functional Requirements	Comments on rationale for tracing and coverage
TOE Objectives		
O.AUDIT_GENERATION: The TOE will provide the capability to detect and create records of security relevant events associated with users	FAU_GEN.1	FAU_GEN.1 defines the set of events that the TOE must be capable of recording and the information that must be contained in the audit record for each auditable event.
	FAU_GEN.2	FAU_GEN.2 ensures the identity of the user that caused an auditable event is included in the audit record information.
O.CORRECT_ TSF_OPERATION: The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.	FPT_TST.1	FPT_TST.1 requires a set of tests to be run on the TSF components that are not protected by the TOE's media protection services to ensure its integrity, and to perform operational tests on the TOE's cryptographic library as required for its FIPS 140-2 certification.
	FCS_COP.1(4)	FCS_COP.1(4) ensures the functionality of the SHA-1 hash function when used for some of the integrity tests in FPT_TST.1
O.DISPLAY_BANNER: The TOE will display an advisory warning regarding use of the TOE.	FTA_TAB.1	FTA_TAB.1 meets this objective by requiring the TOE display a banner, defined during installation, before a user authenticates.
O.MANAGE: The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FMT_MSA.1	FMT_MSA.1 requires that the ability to modify the security attributes for the On-the-Fly Decryption/Encryption SFP be restricted to the Client Administrator.
	FMT_MSA.2	FMT_MSA.2, supporting the cryptographic operations ensure only secure values are accepted for security attributes, verified by the FIPS 140-2 certification.
	FMT_MSA.3	FMT_MSA.3 defines the default value for the On-the-Fly Decryption/Encryption SFP to be permissive for new partitions. By knowing this default, Client Administrators can change it using FMT_MSA.1 as necessary.

Security Objective	Security Functional Requirements	Comments on rationale for tracing and coverage
	FMT_MOF.1	FMT_MOF.1 requires the ability to restrict performing the initial encryption (or decryption by turning it off) on hard disk and removable storage partitions to Client Administrators.
	FMT_MTD.1	FMT_MTD.1 requires the ability to restrict the ability to manipulate and view TOE contents to Client Administrators and users for changing their own passwords.
	FMT_SMF.1	FMT_SMF.1 requires the TOE to provide a mechanism to perform the required management functions.
	FMT_SMR.1	FMT_SMR.1 requires the TOE to support the role of Client Administrator in addition to its regular users.
O.MEDIASEC: The TSF must be able to protect the Client Computer media assets on the Client Administrator-specified hard disk partitions and removable storage devices, using encryption.	FMT_MOF.1	FMT_MOF.1 requires the ability to restrict performing the initial encryption (or decryption by turning it off) on hard disk and removable storage partitions to Client Administrators. This is the function required to meet the objective.
	FCS_COP.1(1)	FCS_COP.1(1) requires the TOE to perform the AES in CBC mode symmetric encryption function using a FIPS 140-2 level 1 certified cryptographic library. The TOE uses this cryptographic operation to encrypt and decrypt the data on the storage partitions.
O.PARTIAL_SELF_PROTECTION: The TSF will maintain a domain for its own execution, and implement an architecture and mechanisms that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces .	FPT_RVM.1(1)	FPT_RVM.1(1) ensures that the TSF makes policy decisions on all interfaces that perform operations on subjects and objects that are scoped by the policies. Without this non-bypassability requirement, the TSF could not be relied upon to completely enforce the security policies, since an interface(s) may otherwise exist that would provide a user with access to TOE resources (including TSF data and executable code) regardless of the defined policies. This includes controlling the accessibility to interfaces, as well as what access control is provided within the interfaces.

Security Objective	Security Functional Requirements	Comments on rationale for tracing and coverage
	FPT_SEP_TOE_EXP.1	FPT_SEP_TOE_EXP.1 ensure the TSF provides a domain that protects itself from untrusted users. If the TSF cannot protect itself it cannot be relied upon to enforce its security policies. The explicitly specified version was used to distinguish the aspects of FPT_SEP provided by the TOE vs. the aspects provided by the IT environment.
	FCS_CKM.1	FCS_CKM.1 ensures good keys are used for the ECC encryption process (FCS_COP.1(2)).
	FCS_CKM.4	FCS_CKM.4 ensures FIPS 140-2 compliant key destruction to support key lifecycle management.
	FCS_COP.1(2)	FCS_COP.1(2) ensures sound cryptographic mechanisms are used for the ECC encryption of the UPC. This cryptographic function is part of the processing sequence the TOE uses to protect itself from being bypassed, interfered with, or tampering, as described in Section 6.6.
	FCS_COP.1(3)	FCS_COP.1(3) ensures cryptographically sound random numbers are used for the cryptographic operation that are part of the processing sequence the TOE uses to protect itself from being bypassed, interfered with, or tampering, as described in Section 6.6.
	FCS_COP.1(4)	FCS_COP.1(4) ensures a sound SHA-1 hash function is used for the cryptographic operations that are part of the processing sequence the TOE uses to protect itself from being bypassed, interfered with, or tampering, as described in Section 6.6. The SHA-1 hash is used to support the integrity checks of the self tests required by FPT_TST.1.
	FCS_COP.1(5)	FCS_COP.1(5) ensures compliance with the integrity requirements of FIPS 140-2.

Security Objective	Security Functional Requirements	Comments on rationale for tracing and coverage
O.PARTIAL_TOE_ACCESS: The TOE will provide mechanisms that control user's logical access to the TOE Client Console and to the TOE mechanism that allows the Client Computer to start-up and make protected data available to the Client Computer users.	FIA_AFL.1	FIA_AFL.1 provides a detection mechanism for unsuccessful authentication attempts for both implementations of the I&A mechanism, logging onto the operating system, and accessing the Client Console interface application. The requirement enables the number of failed attempts, defined during installation, that causes the logon mechanism to delay for 1 minute, making an attempt to guess a password using a brute force attempt impractical.
	FIA_SOS.1	FIA_SOS.1 requires a mechanism to enforce complexity requirements on passwords, ensuring users have passwords that are difficult to guess through a brute force attack.
	FIA_UAU.2 and FIA_UAU_TOE_EXP.2	FIA_UAU.2 requires a mechanism that is enforced as part of the client start-up (boot process) that requires each user to authenticate before the Client Computer starts up. FIA_UAU_TOE_EXP.2 requires a mechanism that is enforced for each user's access to the Client Console application program interface.
	FIA_UAU.7	FIA_UAU.7 requires the TOE to echo back a character that obscures the passwords entered on the logon screen, preventing unauthorized users from seeing authentication data on the screen.
	FIA_UID.2 and FIA_UID_TOE_EXP.2	Same as FIA_UAU.2 and FIA_UAU_TOE_ENV.2
O.TRANSPARENT_ENFORCED_ ACCESS; The TSF must be able to provide authorized users and system processes read and write access to the Client Computer encrypted partitions in a manner that is transparent to users to ensure the mechanism is always invoked and the data is available to the system, authorized users, and applications and is encrypted when not in use and stored on the encrypted partitions.	FDP_IFC.2	FDP_IFC.2 requires the information flow control policy that is enforced on all information flowing between processes that access the client hard disk encrypted partitions and removable storage encrypted files, as required for this objective.
	FDP_IFF.1	FDP_IFF.1 requires a data protection mechanism that acts on all data that is read from or written to the encrypted partitions media. Requiring data from the media (reading it) to be decrypted so it's accessible to users and data sent to the media (writing it) to be encrypted so the information is protected when not in use.

Security Objective	Security Functional Requirements	Comments on rationale for tracing and coverage
	FCS_COP.1(1)	FCS_COP.1(1) requires a the FIPS 140-2 cryptographic library that implements the Cryptographic Support Function includes performing AES in CBC mode encryption/decryption for the initial encryption/terminal decryption and on-the-fly encryption/decryption
IT Environment Objectives		
OE.AUDIT_SUPPORT: The IT environment will provide the capability to view audit information, and will protect the stored audit records from unauthorized modification and deletion, and will provide a timestamp for the audit records.	FAU_SAR.1	FAU_SAR.1 ensures the IT environment provides a mechanism for reading the audit records generated by the TOE. This is required for practical purposes to mitigate the threat of unidentified actions.
	FAU_STG.1	FAU_STG.1 ensures the IT environment protects the audit records generated by the TOE from unauthorized deletion or modification since they are stored in a file on the operating system.
OE.PARTIAL_TOE_PROT: The TSF Environment shall provide virtual memory management, execution rings for executing user software and kernel processes to protect the TOE processes from interference and tampering, and file protection to prevent unauthorized access and modifications to TOE.	FPT_AMT.1	FPT_AMT.1 since the TOE is a software component and requires itself to perform self-tests, the IT environment must also be able to perform some self tests to ensure the correct operation of the abstract machine that underlies the TSF.
	FPT_RVM.1(2)	FPT_RVM.1(2) since the TOE is software it requires its platform to prevent bypassing the TSF interfaces through unauthorized use of the platform interfaces.
	FPT_SEP_ENV_EXP.1	FPT_SEP_ENV_EXP.1 since the TOE is software it requires its platform to also provide domain separation by providing execution rings for the TOE kernel processes, separate from user processes and general process management and separation support by the operating system.
OE.TIMESTAMP: The TOE computing platform will provide reliable time.	FPT_STM.1	FPT_STM.1 since the TOE is software it must receive a timestamp for its audit records and a clock for the logon delay mechanism.

Security Objective	Security Functional Requirements	Comments on rationale for tracing and coverage
OE.TOE_ENVIR_ACCESS: The IT environment will provide the capability to control users' logical access to the Client Computer after its startup.	FIA_UAU_ENV_EXP.2	FIA_UAU_ENV_EXP.2 for access to the Client Computer and its protected resources, since the TOE only authenticates the initial user who starts the computer, the Client Computer operating system must authenticate all subsequent users. Note: the TSF provides a second authentication process for access to its Client Console interface, as specified in FIA_UAU_ENV_EXP.2
	FIA_UID_ENV_EXP.2	FIA_UID_ENV_EXP.2 for access to the Client Computer and its protected resources, since the TOE only identifies the initial user who starts the computer, the Client Computer operating system must identify all subsequent users. Note: the TSF provides a second identification process for access to its Client Console interface, as specified in FIA_UID_ENV_EXP.2.

Table 14 Reverse mapping of SFRs to Security Objectives

This table has been provided to confirm that all security functional requirements map to at least one Security Objective.

SFR ID	TOE Security Objective
FAU_GEN.1	O.AUDIT_GENERATION
FAU_GEN.2	O.AUDIT_GENERATION
FCS_CKM.1	O.PARTIAL_SELF_PROTECTION
FCS_CKM.4	O.PARTIAL_SELF_PROTECTION
FCS_COP.1(1)	O.MEDIASEC
	O.TRANSPARENT_ENFORCED_ACCESS
FCS_COP.1(2)	O.PARTIAL_SELF_PROTECTION
FCS_COP.1(3)	O.PARTIAL_SELF_PROTECTION
FCS_COP.1(4)	O.CORRECT_ TSF_OPERATION
	O.PARTIAL_SELF_PROTECTION
FCS_COP.1(5)	O.PARTIAL_SELF_PROTECTION

SFR ID	TOE Security Objective
FDP_IFC.2	O.TRANSPARENT_ENFORCED_ACCESS
FDP_IFF.1	O.TRANSPARENT_ENFORCED_ACCESS
FIA_AFL.1	O.PARTIAL_TOE_ACCESS
FIA_SOS.1	O. PARTIAL_TOE_ACCESS
FIA_UAU.2	O. PARTIAL_TOE_ACCESS
FIA_UAU_TOE_EXP.2	O. PARTIAL_TOE_ACCESS
FIA_UAU.7	O. PARTIAL_TOE_ACCESS
FIA_UID.2	O. PARTIAL_TOE_ACCESS
FIA_UID_ENV_EXP.2	O. PARTIAL_TOE_ACCESS
FMT_MSA.1	O.MANAGE
FMT_MSA.2	O.MANAGE
FMT_MSA.3	O.MANAGE
FMT_MOF.1	O.MANAGE
	O.MEDIASEC
FMT_MTD.1	O.MANAGE
FMT_SMF.1	O.MANAGE
FMT_SMR.1	O.MANAGE
FPT_RVM.1(1)	O.PARTIAL_SELF_PROTECTION
FPT_SEP_TOE_EXP.1	O.PARTIAL_SELF_PROTECTION
FPT_TST.1	O.CORRECT_ TSF_OPERATION
FTA_TAB.1	O.DISPLAY_BANNER
FAU_SAR.1	OE.AUDIT_SUPPORT
FAU_STG.1	OE.AUDIT_SUPPORT
FIA_UAU_ENV_EXP.2	OE.TOE_ENVIR_ACCESS
FIA_UID_ENV_EXP.2	OE.TOE_ENVIR_ACCESS
FPT_AMT.1	OE.PARTIAL_TOE_PROT

SFR ID	TOE Security Objective
FPT_RVM.1(2)	OE.PARTIAL_TOE_PROT
FPT_SEP_ENV_EXP.1	OE.PARTIAL_TOE_PROT
FPT_STM.1	OE.TIMESTAMP

8.2.1 ASSURANCE RATIONALE

Evaluation Assurance Level 4 (EAL) 4 augmented with ALC_FLR.3 was chosen because it provides appropriate assurance measures for the expected application of the product. EAL4 augmented with ALC_FLR.3 ensures a product is methodically designed, tested, and reviewed with maximum assurance from positive security engineering based on good commercial development practices. It also requires a moderate to high level of independently assured security. The security assurance requirement AVA_VLA.2 includes an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

As appropriate for selection of EAL4 augmented with ALC_FLR.3 for the expected uses of the TOE, some confidence in correct operation is required, but the threats to security are not viewed as serious. Independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

8.2.2 EXPLICITLY STATED REQUIREMENTS RATIONALE

The table below presents the rationale for each of the explicit requirements found in this ST. All explicit requirements are closely modeled on existing CC requirements.

Table 15 Rationale for Explicit Requirements

Explicit Requirement	Identifier	Rationale
FIA_UAU_TOE_EXP.2	O. PARTIAL_TOE_ACCESS	FIA_UAU.2 requires users to be authenticated prior to accessing the Client Computer. However, this SFR requires users to be authenticated a second time prior to accessing the Client Console Interface to the TOE. It is modeled on FIA_UAU.2. CC Part 2 does not include an SFR that requires users to be authenticated a second time to access a TOE interface.
FIA_UID_TOE_EXP.2	O. PARTIAL_TOE_ACCESS	FIA_UID.2 requires users to be Identified prior to accessing the Client Computer. However, this SFR requires users to be identified a second time prior to accessing the Client Console Interface to the TOE. It is modeled on FIA_UID.2. CC Part 2 does not include an SFR that requires users to be identified a second time to access a TOE interface.

Explicit Requirement	Identifier	Rationale
FPT_SEP_TOE_EXP.1	TSF partial domain separation	Basic Robustness Consistency Guidance, Instruction 2 states that the domain separation requirements addressed by the TOE be explicitly stated. The requirement is modeled on FPT_SEP.1 and modified to reflect to cooperative relationship between the TOE and its platform. As with FPT_SEP.1 this explicit requirement has no dependencies.
FIA_UAU_ENV_EXP.2	OE.TOE_ENVIR_ACCESS	This requirement ensures users must authenticate to the environment via the Windows logon after a successful Pre-boot Authentication has been performed by the TOE. This requirement is model on FIA_UAU.2.
FIA_UID_ENV_EXP.2	OE.TOE_ENVIR_ACCESS	This requirement ensures users must identify themselves to the environment using the Windows logon after a successful Pre-boot Authentication has been performed by the TOE. This requirement is model on FIA_UID.2.
FPT_SEP_ENV_EXP.1	TSF Environment partial domain separation	This requirement is the compliment to the FPT_SEP_TOE_EXP.1, and is also modeled on Basic Robustness Consistency Guidance.

8.2.3 DEPENDENCIES

The table below shows the dependencies between the functional requirements. All dependencies are satisfied. Dependencies that are satisfied by hierarchical components are denoted by an (H) following the dependency reference. (E) designates that the SFR is for the IT Environment, (T) designates that the SFR is for the TOE.

Table 16 TOE Dependencies Satisfied

Item	SFR ID	SFR Title	Dependencies	Item Reference
1	FAU_GEN.1	Audit data generation	FPT_STM.1	8 (E)
2	FAU_GEN.2	User identity association	FAU_GEN.1	1
			FIA_UID.1	16(H) & 17(H)
3	FCS_CKM.1	Cryptographic key generation	FCS_COP.1	6
			FCS_CKM.4	4
			FMT_MSA.2	19
4	FCS_CKM.4	Cryptographic key destruction	FCS_CKM.1	3
			FMT_MSA.2	19
5	FCS_COP.1(1)	Cryptographic operation (AES)	FCS_CKM.1	See note in Table 18

Item	SFR ID	SFR Title	Dependencies	Item Reference
6	FCS_COP.1(2)	Cryptographic operation (ECC of UPC)	FCS_CKM.1	3
			FCS_CKM.4	4
			FMT_MSA.2	19
7	FCS_COP.1(3)	Cryptographic operation (RNG)	FCS_CKM.1	See note in Table 18
8	FCS_COP.1(4)	Cryptographic operation (Secure Hash)	FCS_CKM.1	See note in Table 18
8A	FCS_COP.1(5)	Cryptographic operation (Hash MAC)	FCS_COP.1	8
9	FDP_IFC.2	Complete information flow control	FDP_IFF.1	10
10	FDP_IFF.1	Simple security attributes	FDP_IFC.1	9(H)
			FMT_MSA.3	20
11	FIA_AFL.1	Authentication failure handling	FIA_UAU.1	13(H) & 14 (H)
12	FIA_SOS.1	Verification of secrets	None	None
13	FIA_UAU.2	User authentication before any action (User Access to Client Computer)	FIA_UID.1	16(H)
14	FIA_UAU_TOE_EXP.2	User authentication before any action (Client console)	FIA_UID_TOE_EXP.2	17
15	FIA_UAU.7	Protected authentication feedback	FIA_UAU.1	13(H) & 14(H)
16	FIA_UID.2	User identification before any action (User Access to Client Computer)	None	None
17	FIA_UID_TOE_EXP.2	User identification before any action (Client console)	None	None
18	FMT_MSA.1	Management of security attributes	FDP_IFC.1	9(H)
			FMT_SMR.1	24
			FMT_SMF.1	23
19	FMT_MSA.2	Secure security attributes	ADV_SPM.1	EAL4+
			FDP_IFC.1	9(H)
			FMT_MSA.1	18
			FMT_SMR.1	24
20	FMT_MSA.3	Static attribute initialization	FMT_MSA.1	18
			FMT_SMR.1	24
21	FMT_MOF.1	Management of security functions behaviour	FMT_SMR.1	24
			FMT_SMF.1	23
22	FMT_MTD.1	Management of TSF data	FMT_SMR.1	24

Item	SFR ID	SFR Title	Dependencies	Item Reference
			FMT_SMF.1	23
23	FMT_SMF.1	Specification of management functions	None	None
24	FMT_SMR.1	Security roles	FIA_UID.1	16(H) & 17(H)
25	FPT_RVM.1(1)	Non-bypassability of the TSP (TOE)	None	None
26	FPT_SEP_TOE_EXP.1	TSF partial domain separation:	None	None
27	FPT_TST.1	TSF testing	FPT_AMT.1	5(E)
28	FTA_TAB.1	Default TOE access banners	None	None

Table 17 IT Environment Dependencies are Satisfied

Item	SFR ID	SFR Title	Dependencies	Item Reference
1E	FAU_SAR.1	Audit review	FAU_GEN.1	1(T)
2E	FAU_STG.1	Protected audit trail storage	FAU_GEN.1	1(T)
3E	FIA_UAU_ENV_EXP.2	User authentication before any action (Client Computer O/S)	FIA_UID_ENV_EXP.2	4(E)
4E	FIA_UID_ENV_EXP.2	User identification before any action (Client Computer O/S)	None	None
5E	FPT_AMT.1	Abstract machine testing	None	None
6E	FPT_RVM.1(2)	Non-bypassability of the TSP (Platform)	None	None
7E	FPT_SEP_ENV_EXP.1	TSF Environment partial domain separation	None	None
8E	FPT_STM.1	Reliable time stamps	None	None

8.2.4 RATIONALE FOR DEPENDENCIES NOT SATISFIED

The following table provides the rationale for dependencies that are not satisfied.

Table 18 Dependencies Not Satisfied

SFR	Dependency not satisfied	Rationale
FCS_COP.1(1)	FCS_CKM.1	The dependency for generating the key for this cryptographic operation is performed during the installation process. The process is covered in ADO_IGS.1. The verification of this key generation is covered in the TOE’s FIPS 140-2 level 1 certification. The integrity of the key during the installation process is addressed by FPT_TST.1
FCS_COP.1(3)	FCS_CKM.1	The RNG cryptographic operation does not use a key.

SFR	Dependency not satisfied	Rationale
FCS_COP.1(4)	FCS_CKM.1	The SHA-1 cryptographic operations do not use a key.

8.2.5 RATIONALE THAT IT SECURITY REQUIREMENTS ARE INTERNALLY CONSISTENT

The IT Security Requirements are internally consistent. There are no requirements that conflict with one another. When different IT security requirements apply to the same event, operation, or data there is no conflict between the security requirements. The requirements mutually support each other to apply to the event, operation, or data.

For auditing, FAU_GEN.1, Audit data generation, details auditable events generated by the TSF and consistent with the security functions claimed by the TOE. The IT environment provides protection of these audit records in FAU_STG.1 and a facility to read or process the records in FAU_SAR.1, and reliable time stamps required in FPT_STM.1. Since the TOE puts the audit records in the operating system event file, providing a means to process the records outside of the TOE is reasonable.

The FIA* requirements compose the I&A security function with the IT environment providing the clock to measure the logon delay for the failure mechanism and authentication for users after Client Computer start-up. The same I&A function is implemented at Client Computer start-up and to control access to the Client Console interface. The I&A function at client start-up supports the aspect of the TOE Self Protection function that uses a processing sequence to protect itself from being bypassed, interfered with, or tampering.

FPT_RVM.1(1) and FPT_SEP_TOE_EXP.1 work in concert with the IT environment FPT_RVM.1(2) FPT_SEP_ENV_EXP.1 to provide non-bypassability and domain separation. The TOE’s FPT_TST.1 supports integrity checks for the software not covered by the TOE’s own protection services defined in FDP_IFF.2 and FDP_IFC.1.

The cryptographic operations support the TOE functions and do not provide external user services.

The following table shows the management specifications are complete and consistent with the requirements:

Table 19 Management Specifications Complete

ST Functional Component ID	CC recommendation	Application in ST
FAU_GEN.1	None	N/A
FAU_GEN.2	None	N/A
FCS_CKM.1	the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption).	These are not configurable parameters in the TOE.

ST Functional Component ID	CC recommendation	Application in ST
FCS_CKM.4	the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption).	These are not configurable parameters in the TOE.
FCS_COP.1	None	N/A
FDP_IFC.2	None	N/A
FDP_IFF.1	a) The enabling or disabling of the monitoring function. b) Modification of the maximum capacity at which the monitoring occurs.	a) Client Administrator via FMT_MOF.1 b) not a parameter in the TOE.
FIA_AFL.1	Management for the threshold for unsuccessful authentication attempts Management of actions to be taken in the event of an authentication failure.	1. Policy Administrator during the installation process. 2. not a configurable parameter.
FIA_SOS.1	The management of the metric used to verify secrets	Policy Administrator during the installation process
FIA_UAU.2*	a) management of the authentication data by an administrator; b) management of the authentication data by the user associated with this data.	a) Client Administrator via FMT_MTD.1 b) user via FMT_MTD.1
FIA_UAU.7	None	N/A
FIA_UID.2*	the management of the user identities	Client Administrator via FMT_MTD.1
FMT_MSA.1	Managing the group of roles that can interact with the security attributes	Policy Administrator during the installation process.
FMT_MSA.2	None	N/A
FMT_MSA.3	a) Managing the group of roles that can interact with the security attributes b) managing the permissive or restrictive setting of default values for a given access control SFP.	a) Policy Administrator during the installation process b) not a configurable parameter in the TOE.
FMT_MOF.1	Managing the group of roles that can interact with the TSF data	not a configurable parameter in the TOE.
FMT_MTD.1	Managing the group of roles that can interact with the TSF data	not a configurable parameter in the TOE.
FMT_SMF.1	None	N/A

ST Functional Component ID	CC recommendation	Application in ST
FMT_SMR.1	Managing the group of users that are part of a role.	Policy Administrator during the installation process
FPT_RVM.1	(based on FPT_RVM.1) None	N/A
FPT_SEP_TOE_EXP.1	None	N/A
FPT_TST.1	a) management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions; b) management of the time interval if appropriate.	a) not a configurable parameter in the TOE. b) not a configurable parameter in the TOE.
FTA_TAB.1	maintenance of the banner by the authorised administrator.	Policy Administrator during the installation process.

8.3 TOE Summary Specification Rationale

8.3.1 IT SECURITY FUNCTIONS RATIONALE

Table below shows that the IT security functions in the TOE Summary Specification (TSS) implement all of the TOE Security Functional Requirements.

Table 20 Mapping SFRs to TOE Summary Specification Rationale

SFR	TOE Security Function	Rationale
FAU_GEN.1	Security Audit	The logging mechanism in Security Audit provides the required audit records.
FAU_GEN.2	Security Audit	The logging mechanism in Security Audit includes the user’s identity for applicable auditable events it records.
FCS_CKM.1	Cryptographic Support	The FIPS 140-2 cryptographic library that implements the Cryptographic Support Function includes key generation for the ECC key pairs for encrypting the UPC. This provides support the TOE Protection security function.
FCS_CKM.4	Cryptographic Support	The FIPS 140-2 cryptographic library that implements the Cryptographic Support Function includes key destruction for all keys.
FCS_COP.1(1)	Cryptographic Support	The FIPS 140-2 cryptographic library that implements the Cryptographic Support Function includes performing AES in CBC mode encryption/decryption for the initial encryption and on-the-fly decryption/encryption, for the Data Protection and Security Management security functions.

SFR	TOE Security Function	Rationale
FCS_COP.1(2)	Cryptographic Support	The FIPS 140-2 cryptographic library that implements the Cryptographic Support Function includes performing ECC encryption decryption of the UPC key using the key pairs in FCS_CKM.1. This provides support the TOE Protection function.
FCS_COP.1(3)	Cryptographic Support	The FIPS 140-2 cryptographic library that implements the Cryptographic Support Function includes a random number generator to support other cryptographic operations and for generating the UPC used to support the TOE Protection function.
FCS_COP.1(4)	Cryptographic Support	The FIPS 140-2 cryptographic library that implements the Cryptographic Support Function includes the SHA-1 secure hash function. SHA-1 is used to support the cryptographic operations, performing a secure hash on the WEK and UPC, and for integrity checks for the self-testing mechanism to support the TOE Protection security function.
FDP_IFC.2	Data Protection	The data protection mechanism is implemented at the device driver level for each "encrypted partition" of the hard disk and removable storage. The mechanism is applied to all processes that access the media and for all information (data) between the processes and the media.
FCS_COP.1(5)	Cryptographic Support	The FIPS 140-2 cryptographic library that implements the Cryptographic Support Function includes the HMAC secure Message Authentication Code. HMAC is used indirectly in the implementation of the PBKDF2 function (for deriving keys from passwords)
FDP_IFF.1	Data Protection	The data protection mechanism acts on the read and write instructions device drivers use to get and send data to the media. When getting data from the media (reading it) the data protection mechanism (using the cryptographic support) decrypts the information so it's accessible to users. When sending data to the media (writing it) the data protection mechanism (using the cryptographic support) encrypts the information so it's protected when not in use. The data protection mechanism uses an IV that is generated by a PRNG that is seeded with the relative sector address of the "encrypted partition" or the block offset from the head of the encrypted data in the hard disk encryption and removable storage encryption cases respectively to support the cryptographic processes.
FIA_AFL.1	Identification and Authentication	The identification and authentication function includes a mechanism the delays the logon function for 1minute based on the number of incorrect attempts specified during installation.
FIA_SOS.1	Identification and Authentication	The identification and authentication function includes a mechanism that puts constraints on the passwords users create for themselves, in the management function. These constraints ensure that each authentication secret meets the complexity requirements specified at installation.

SFR	TOE Security Function	Rationale
FIA_UAU.2	Identification and Authentication	The identification and authentication function is implemented in two instances: The first is for users' access to the Client Computer. The authentication mechanism is called immediately following the identification mechanism and is part of the Client Computer "start-up" (boot) process, ensuring users are identified and authenticated before the computer can start.
FIA_UAU_TOE_EXP.2	Identification and Authentication	This explicit requirement of the identification and authentication function is implemented when users access the Client Console TOE application process. Each user must successfully be identified and authenticated before any TSF-mediated actions can occur from that Client Console TOE interface.
FIA_UAU.7	Identification and Authentication	The identification and authentication function obscures the password typed in the logon screen for the authentication process. This applies to both instances of the identification and authentication mechanism.
FIA_UID.2	Identification and Authentication	Same as FIA_UAU.2
FIA_UID_TOE_EXP.2	Identification and Authentication	Same as FIA_UAU_TOE_EXP.2
FMT_MSA.1	Security Management	The security management function is implemented through the Client Console TOE application interface. Through this interface Client Administrators can perform the initial encryption or decryption process which sets the attributes for applying the on-the fly decryption SFP on the encrypted partitions.
FMT_MSA.2	Security Management	The security management function ensures only secure values are accepted for security attributes by using the FIPS 140-2 cryptographic support function.
FMT_MSA.3	Security Management	The security management function mechanism requires initial encryption be performed on new partitions added to the Client Computer before the on-the-fly decryption/encryption SFP applies to them. This is effectively providing permissive default values for the security attributes used to enforce the SFP.
FMT_MOF.1	Security Management	The security management function is implemented through the Client Console TOE application interface. Through this interface Client Administrators can perform the initial encryption or decryption process which sets the attributes for applying the on-the fly decryption SFP on the encrypted partitions.
FMT_MTD.1	Security Management	The security management function is implemented through the Client Console TOE application interface. Through this interface Client Administrators can add and remove registered users, change passwords, and view the evaluated configuration settings established in the installation process. Through this interface registered users can change their password.

SFR	TOE Security Function	Rationale
FMT_SMF.1	Security Management	The security management function is implemented through the Client Console TOE application interface that provides the mechanism to perform the management functions.
FMT_SMR.1	Security Management	The security management function recognizes two distinct roles, Client Administrator and registered user. Depending on their role the appropriate Client Console interface is provided.
FPT_RVM.1(1)	TOE Protection	As described in detail in Section 6.6, the TOE Protection function uses a combination of architecture and security mechanisms to work in concert with its platform to ensure the TSF cannot be bypassed.
FPT_SEP_TOE_EXP.1	TOE Protection	As described in detail in Section 6.6, the TOE Protection function uses a combination of architecture and security mechanisms to work in concert with its platform to ensure the TSF cannot be corrupted or otherwise compromised.
FPT_TST.1	TOE Protection	The TOE Protection function includes a self-testing mechanism to ensure the integrity of the portions of the TOE not protected by the encryption of the hard disk media, and to verify the operation of cryptographic functions as specified in the FIPS 140-2 level 1 certification.
FTA_TAB.1	Access Banner	The access banner function implements a mechanism that displays a message defined during the installation process on each logon screen presented.
IT Environment SFRs required to support the TOE Security Functions		
FAU_SAR.1	Security Audit	The IT environment operating system provides an interface to review the audit records, a practical aspect of the security audit function.
FAU_STG.1	Security Audit	The IT environment operating system provides an access control mechanism on the audit file to protect it from unauthorized deletion or modification.
FIA_UAU_ENV_EXP.2	Identification and Authentication	The IT environment provides the mechanism to control the users’ access to the Client Computer after its startup, and therefore controlling access to the protected data.
	Security Management	The IT environment, by providing the logon function to users on the Client Computer after its startup, provides the user identifier to the TOE to determine whether that user is a registered user and if not, offered the opportunity to register with the TSF.
FIA_UID_ENV_EXP.2	Identification and Authentication	Same as FIA_UAU_ENV_EXP.2
	Security Management	Same as FIA_UAU_ENV_EXP.2
FPT_AMT.1	TOE Protection	The IT environment provides a tool to verify the integrity of the underlying platform since the TOE is a software application and depends on its platform for operation.

SFR	TOE Security Function	Rationale
FPT_RVM.1(2)	TOE Protection	Since the TOE is a software application the IT environment platform provides file protections and process support to help ensure the TOE interfaces cannot be bypassed.
FPT_SEP_ENV_EXP.1	TOE Protection	Since the TOE is a software application the IT environment platform provides virtual memory management and user mode and kernel mode execution rings to support domain separation.
FPT_STM.1	Security Audit	The IT environment operating system provides the timestamp for the audit records of the Security Audit function and relies on its underlying hardware to provide the clock for the timestamp.
	Identification and Authentication	The IT environment platform provides the clock for measuring the 1 minute delay for the authentication failure mechanism of the identification and authentication function

8.3.2 RATIONALE FOR ASSURANCE MEASURES TO SECURITY ASSURANCE REQUIREMENTS

Please see the table in Section 6.9 for the tracing from Security Assurance Measures to Security Assurance Requirements and the rationale of how the Assurance Measures satisfy the assurance requirements.

8.4 Strength of Function Claims

Part 1 of the CC defines “strength of function” in terms of the minimum efforts assumed necessary to defeat the expected security behavior of a TOE security function. There are three strength of function levels defined in Part 1: SOF-basic, SOF-medium and SOF-high. SOF-medium is the strength of function level chosen for this ST. SOF-medium states, “A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.”

The rationale for choosing SOF-medium was to be consistent with the assurance requirements included in this ST; namely the environment is one where the potential attacker is proficient with access to specialized equipment and public information, consistent with a Common Criteria Level of Evaluation of EAL4 augmented with ALC_FLR.3. Specifically, AVA_VLA.2 requires that the TOE be resistant to an attacker with a low attack potential, this is satisfied by SOF-medium. Consequently, the metrics (password) chosen for inclusion in this ST for this TOE were determined to be acceptable for SOF-medium.

The one security function based on probabilistic methods is identified in Section 6.4, “Identification and Authentication” and applies to FIA_SOS.1 to meet the objective O.PARTIAL_TOE_ACCESS. The specific “strength” required of the methods used provide difficult-to-guess passwords are defined in the FIA_SOS.1 password policy.

8.5 List of Acronyms

CC	Common Criteria
EAL	Evaluation Assurance Level
GEFR	GuardianEdge Framework
GEFS	GuardianEdge File System
GEHD	GuardianEdge Hard Disk Encryption
GMBR	GuardianEdge Master Boot Record
GPBA	GuardianEdge Pre-Boot Authentication
GERS	GuardianEdge Removable Storage Encryption
IT	Information Technology
MBR	Master Boot Record
OSP	Organizational Security Policy
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSFI	TSF Interface
TSP	TOE Security Policy
WEK	Workstation Encryption Key

9.0 Glossary

This section defines the Common Criteria terms. Not all of these terms are used in this document.

Assignment The specification of an identified parameter in a component.

Assurance Grounds for confidence that an entity meets its security objectives.

Attack potential The perceived potential for success of an attack, should an attack be launched, expressed in terms of a threat agent’s expertise, resources and motivation.

Augmentation The addition of one or more assurance component(s) from Part 3 to an EAL or assurance package.

Authentication data Information used to verify the claimed identity of a user.

Authorized user A user who may, in accordance with the TSP, perform an operation.

Bulk Encryption The encryption of large amounts of data. This is as opposed to key encryption.

Class A grouping of families that share a common focus.

Component The smallest selectable set of elements that may be included in a PP, an ST, or a package.

Connectivity The property of the TOE that allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.

Dependency A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.

Element An indivisible security requirement.

Evaluation Assessment of a PP, an ST, or a TOE against defined criteria.

Evaluation Assurance Level (EAL) A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.

Evaluation authority A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.

Evaluation scheme The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.

Extension The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.

External IT entity Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Family A grouping of components that share security objectives but may differ in emphasis or rigor.

Formal Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Human user Any person who interacts with the TOE.

Identity A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Informal Expressed in natural language.

Initial Encryption The encryption of the designated hard disk partitions that follows the installation of GuardianEdge Hard Disk Encryption is called initial encryption. This is as opposed to terminal decryption.

Internal communication channel A communication channel between separated parts of TOE.

Internal TOE transfer Communicating data between separated parts of the TOE.

Inter-TSF transfers Communicating data between the TOE and the security functions of other trusted IT products.

Iteration The use of a component more than once with varying operations.

Key Encryption Encryption of keys for key management purposes. This is as opposed to bulk encryption.

Object An entity within the TSC that contains or receives information and upon which subjects perform operations.

Organizational security policies One or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

Package A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.

Product A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.

Protection Profile (PP) An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Reference monitor The concept of an abstract machine that enforces TOE access control policies.

Reference validation mechanism An implementation of the reference monitor concept that possesses the following properties: it is tamperproof, always invoked, and simple enough to be subjected to thorough analysis and testing.

Refinement The addition of details to a component.

Role A predefined set of rules establishing the allowed interactions between a user and the TOE.

Secret Information that must be known only to authorized users and/or the TSF in order to enforce a specific SFP.

Security attribute Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.

Security Officer Person responsible for setting IT security policies at an organization.

Security Function (SF) A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Function Policy (SFP) The security policy enforced by an SF.

Security objective A statement of intent to counter identified threats and/or satisfy identified organization security policies and assumptions.

Security Target (ST) A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Selection The specification of one or more items from a list in a component.

Semiformal Expressed in a restricted syntax language with defined semantics.

Strength of Function (SOF) A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms.

SOF-basic A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by threat agents possessing a low attack potential.

SOF-medium A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by threat agents possessing a moderate attack potential.

SOF-high A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organized breach of TOE security by threat agents possessing a high attack potential.

Subject An entity within the TSC that causes operations to be performed.

System A specific IT installation, with a particular purpose and operational environment.

Target of Evaluation (TOE) An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

Terminal Decryption Terminal decryption refers to the decryption of encrypted hard disk partitions. In the TOE, only the Client Administrator can perform this task. This is as opposed to initial encryption.

TOE resource Anything useable or consumable in the TOE.

TOE Security Functions (TSF) A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Functions Interface (TSFI) A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.

TOE Security Policy (TSP) A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TOE security policy model A structured representation of the security policy to be enforced by the TOE.

Transfers outside TSF control Communicating data to entities not under control of the TSF.

Trusted channel A means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.

Trusted path A means by which a user and a TSF can communicate with necessary confidence to support the TSP.

TSF data Data created by and for the TOE, that might affect the operation of the TOE.

TSF Scope of Control (TSC) The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

User Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

User data Data created by and for the user that does not affect the operation of the TSF.

10.0 References

[AES] Federal Information Processing Standards Publication 197, *Advanced Encryption Standard*

[AES-MODES] National Institute of Standards – Special Publication 800-38A , *Recommendation for Block Cipher Modes of Operation*, 2001 Edition.

[ECDH] Elliptic Curve Diffie-Hellman (ECDH) algorithm DL/ECKAS-DH1 (Discrete Log/Elliptic Curve Key Agreement Scheme Diffie-Hellman, Version 1) using derivation primitive ECSVDP-DH (Elliptic Curve Secret Value Derivation Primitive, Diffie Hellman Version) from **[IEEE-P1363]**. This algorithm is used with KDF2. See **[KDF2]**.

[HMAC-SHA-1] Federal Information Processing Standards Publication 198, *The Keyed-Hash Message Authentication Code (HMAC)*, 6 March 2002.

[IEEE-P1363] IEEE P1363, *Standard Specifications for Public Key Cryptography*, Draft Version 13, 12 November 1999.

[IEEE-P1363a] IEEE P1363a / D9 (Draft Version 9), *Standard Specifications for Public Key Cryptography: Additional Techniques*, 13 July 2001.

[KDF2] Key Derivation Function 2 (KDF2) algorithm from **[IEEE-P1363a]**.

[PBKDF2] Password-Based Key Derivation Function 2 (PBKDF2) algorithm from PKCS#5.

[RNG] FIPS 186 X generator from Section 3.1.

[SHA-1] Federal Information Processing Standards Publication 180-1, *Secure Hash Standard*, 17 April 1995.