Verdasys®
Digital Guardian™ v6.0.1

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.4

Prepared for:

VERDASYS

Verdasys
404 Wyman Street, Suite 320
Waltham, MA 02451
United States of America
Phone: +1 781 788-8180
Email: info@verdasys.com
http://www.verdasys.com

Prepared by:

Corsec

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America
Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the Verdasys Digital Guardian™ v6.0.1, and will hereafter be referred to as the TOE throughout this document. The TOE is a software-only Enterprise Information Protection (EIP) solution which is deployed in an agent/server configuration. The agent software enforces host-based access control, as well as file and removable media encryption, while the server software provides management, forensic reports, and distribution of agent policies.

1.1 Purpose

This ST is divided into nine sections, as follows:

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

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references:

Table 1 - ST and TOE References

ST Title	Verdasys® Digital Guardian™ v6.0.1 Security Target
ST Version	Version 1.4
ST Author	Corsec Security, Inc.
ST Publication Date	10/2/2012
TOE Reference	Verdasys Digital Guardian Server v6.0.1.0042 Verdasys Digital Guardian Agent v6.0.1.0107
FIPS[1] 140-2 Status	Verdasys Secure Cryptographic Module (VSEC), Level 1, Certificate No. 1607 (Consolidated Certificate No. 0009)

[1] FIPS – Federal Information Processing Standard

1.3 Product Overview

Verdasys® Digital Guardian™ v6.0.1 is a comprehensive Enterprise Information Protection (EIP) solution for workstations and servers running Microsoft Windows or Linux operating systems (OS). EIP enables secure data exchange while providing measures for compliance and risk mitigation. Digital Guardian offers an enterprise-wide, policy-driven, and data-centric approach to information security, enabling organizations to address the risks and challenges brought on by an ever-evolving collaborative and mobilized business environment. It focuses on enforcing security at the data level, using pervasive measures to monitor and react to all types of information flow to and from the computer systems it is intended to protect.

Through its unique architecture, Digital Guardian (DG) reduces the risk of data loss or misuse by its realtime enforcement of corporate security policies, automated encryption of files and emails, and automatic discovery and classification of sensitive data. Digital Guardian protects information at rest, in use, and in motion, mitigating both internal and external risks. Its sophisticated tracking and reporting capabilities provide visibility into how information is used and where it is located. This activity data can then be correlated into actionable intelligence. It can also provide powerful forensic support during investigations into fraud, theft, and malicious activity.

Using Digital Guardian's EIP platform, IT security managers can:

- Discover and classify sensitive data by context and content to gain visibility into how it is used by employees, contractors, partners, and outsourcers.
- Utilize actionable decision support to assess the risk associated with the sharing of sensitive data, enabling managers to make informed business decisions and create effective data security policies.
- Implement automated policy-driven information protection, making users accountable for their actions and resulting in voluntary compliance and increased risk-aware behavior.
- Alert, block, and record high-risk behavior, ultimately preventing costly and damaging data loss incidents.

Figure 1 demonstrates the modules, agent types, supported platforms, and base components of the Digital Guardian framework.

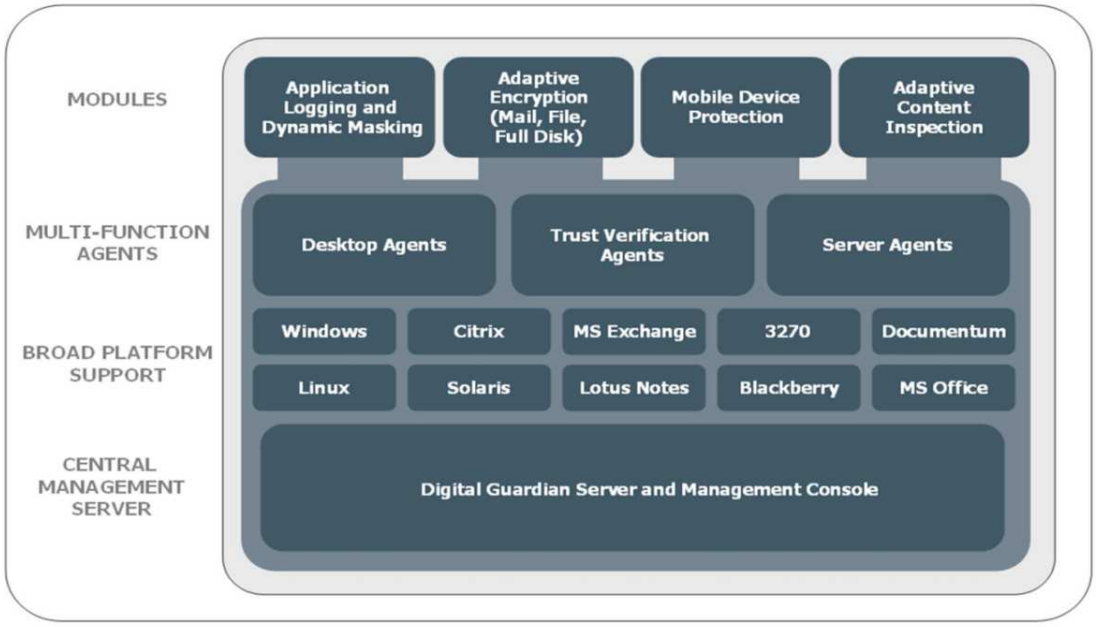

Figure 1 - Digital Guardian Integrated Framework

The Digital Guardian integrated framework offers:

- Comprehensive information protection coverage which is fully functional on or off the corporate network.
- Enterprise-wide visibility into sensitive data location and usage with actionable decision support.
- Centralized policy definition and enforcement that leverages identity, activity, data classification, context, and content analysis.
- Risk-appropriate responses to user activities, including policy-driven warnings, blocking, and alerting, as well as automated encryption of files, emails, and full disks.

At the core of the Digital Guardian architecture is a small, invisible, tamper-resistant agent that is installed on desktops, laptops, and servers, where it is able to continually monitor, collect information on, and mediate all operations performed on protected objects by end-users. Using a low-level kernel-mode driver, the agent is able to inspect all data flows into and out of the protected system. To protect itself from malicious users, the agent software offers resiliency features such as tamper-resistance and invisibility cloaking, thus making it impossible to be detected or tampered with by end-users of the protected system. It also provides fault-tolerance by continuing to enforce policy even when disconnected from the enterprise network, which ensures persistent enforcement of policies on mobile devices which are typically in an offline state and difficult to protect, such as laptops and smart phones.

All data flows are inspected in real-time, and compared against a set of access control rules contained within a policy applied to the user or machine. If the activity matches a particular pattern, a rule is triggered, which results in an action. Rule enforcement actions include: blocking the operation, prompting the user, allowing the operation, alerting, or encrypting the data.

The Digital Guardian Agent (DG Agent) software is capable of two types of rule enforcement: contextual and content-based. Contextual enforcement focuses on the circumstantial aspects of data flow, such as the source and destination of data under inspection, the data's attributes, application(s) involved in the data flow, and the type of operation being performed. Content-based enforcement enables the agent to inspect data payloads in real-time to identify strings of sensitive information such as credit card numbers, social security numbers (SSNs), or any other data that is classified as personally identifiable information (PII).

As a result of its inspection, classification, and enforcement capabilities, the Digital Guardian platform is able to protect against misuse, compromise, or loss of data via mass installation of its multi-function security agent on all workstations and servers across the enterprise. This allows Digital Guardian to monitor and prevent "hard to detect" high-risk user actions such as:

- Writing sensitive data to external media or devices (such as USB[2] memory sticks, CD/DVD[3] discs, etc.)
- Cut/copy/paste operations between applications
- Screen captures, print screen, and printing
- Emailing of content or attachments via either local or web-based email applications
- Transferring data across the network to other systems
- Accessing and interacting with custom or legacy applications

The Digital Guardian Agent oversees transactions at the "point of use", or host, making it capable of protecting data simultaneously across applications, devices, and channels of communication. The Digital Guardian Agent offers the following optional, licensed add-on modules, which extend its protection capabilities:

- **Adaptive File Encryption (AFE)** – Encrypts files in response to rules and events
- **Removable Media Encryption (RME)** – Encrypts files moved to removable media
- **Adaptive Mail Encryption (AME)** – Encrypts file attachments sent by email

[2] USB – Universal Serial Bus
[3] CD/DVD – Compact Disc / Digital Versatile Disc

- **Adaptive Content Inspection (ACI)** – Examines the contents of files and buffers containing strings sensitive information
- **Adaptive Data Inspection (ADI)** – Examines the contents of files for keywords, content patterns, and document similarities
- **Advanced Persistent Threat (APT)** – Detects complex malware behavior patterns and calculates a threat severity and risk score for software based on memory traits
- **Application Compliance (ACM)** – Records and redacts field-level activity in Windows, Web, and 3270 terminal applications
- **Documentum Extension (DTM)** – Monitors and governs user activity performed within EMC Documentum
- **SharePoint Extension (SPT)** – Monitors and governs user activity performed within Microsoft SharePoint
- **User Classification (UC) –** Encompasses three classification modules: Message, Office, and Document
- **Investigation Module (IM) –** Records keystrokes, screen captures, and file captures for use in investigation of suspicious activity

The Digital Guardian Agent is also capable of performing discovery of data at rest, such as files stored on a local hard drive. Files are catalogued according to their sensitivity attributes, which include file extensions, locations, or contents. The agent contains a file scanner, which analyzes drive contents, and based on a set of classification rules, flags the files as sensitive based on their context, or content. Using the AFE module, the agent is capable of scanning local hard disks and performing automatic encryption of files classified as sensitive, or that match a set of conditions specified by a rule. Files are encrypted using a site-wide session key, and can only be decrypted by other machines running the agent software.

To protect sensitive data written to removable media from unauthorized loss or disclosure, the RME module provides encryption features for USB and optical drives. Files can be protected using public and private encryption; public encryption allows any other agent-mediated computer to decrypt the files stored on the removable media; private encryption allows the user to enter a shared secret to be disclosed only to the party with which the media is to be shared. Optionally, a small application can be included on the removable media, which contains the drivers necessary to decrypt the encrypted files on a non-protected machine.

All activity occurring on the agent computer is collected and reported back to the Digital Guardian Management Server (DG Server), where IT security managers can review agent activity through the web-based Digital Guardian Management Console (DGMC). The reporting features offered by the Digital Guardian Management Console provide actionable insight into the security posture of the organization. Using this information, managers can identify the risky behavior occurring within the environment and construct rules governing allowable activity, or activity that constitutes a violation of an organizational security policy. Activity resulting in a rule violation will generate alerts, which can be reviewed by users of the DGMC or subscribed to as email notifications, giving incident responders real-time indication of high-risk activity. Violation alerts, coupled with the forensic data gathered by Digital Guardian Agents, can then be used to aid in an investigation of data breaches or other security-related incidents.

Digital Guardian can also be used in conjunction with the Verdasys Fidelis Appliance/Digital Guardian Network Agents and eDiscovery Agents. The Fidelis Appliance/Network Agent is a Linux-based network device/software agent used to complement Digital Guardian by providing increased visibility into network traffic and events. The e-Discovery Agents are specialized DG Agents which run on a Linux-based server and scan network repositories to identify and catalog sensitive information. The Digital Guardian Management Server recognizes Fidelis Appliance/Network Agents and eDiscovery as specialized agents, from which it receives event and alert data, which are catalogued and stored with other DG events, and can be used to alert security response personnel using Digital Guardian's notification capabilities.

The DG Agent can also be installed on Citrix and Terminal Servers and Blackberry Enterprise Servers, ensuring complete access control of interactive user applications, both remote and mobile, as well as encrypting/monitoring email attachments and user activity.

1.4 TOE Overview

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

1.4.1 Brief Description of the Components of the TOE

The following components comprise the software-only TOE:

- DG Agent
  - DG Agent software (Windows Workstation)
  - DG Agent software (Windows Server)
  - DG Master
  - DG Scanner
  - DG Application Programming Interface (API)
  - AFE add-on module
  - RME add-on module
  - Verdasys Secure Cryptographic Module (VSEC)
- DG Server
  - DG Management Server software
  - DG Management Console

Note: Throughout this document, the term "DG Agent" refers collectively to the client-side components of the TOE, and may also be referred to as "TOE agent", particularly within the Security Problem Description (SPD), Security Objectives, and Rationale. The server-side components, collectively referred to as "DG Server", may also be referred to as "TOE server" in the SPD, Security Objectives, and Rationale.

Figure 2 illustrates the components which make up the TOE and their environmental counterparts:

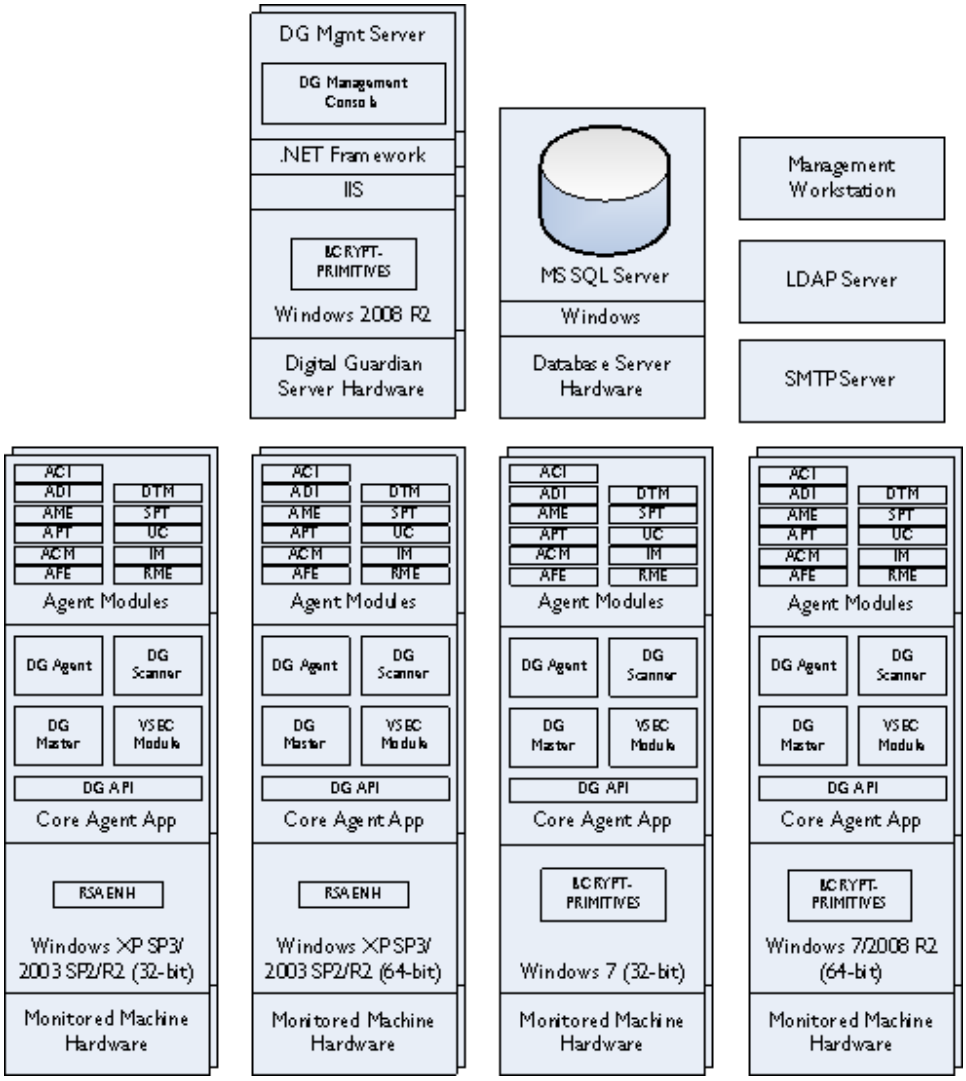

Figure 2 - TOE Environment

The following, previously undefined acronyms appear in the figure above:

- LDAP – Lightweight Directory Access Protocol
- RSAENH – Microsoft Windows Enhanced Cryptographic Provider (Windows XP SP3/Server 2003 SP2/R2)
- SMTP – Simple Mail Transfer Protocol
- SP – Service Pack
- SQL – Structured Query Language

The TOE consists of a software-based, client/server architecture, with a centralized *DG Management Server* and *DG Agents* distributed throughout the workstations and servers within an enterprise. The *DG Agent* comprises a user-mode application, *DG Agent* is a term used to collectively refer to all client-side components; however, it more specifically refers to the user-mode application used for retrieving policies from and sending logs to the *DG Server*, as well as prompting end-users with warning or informational messages when rules are triggered. *DG Agent* depends on four other components to enforce access control policies:

- the API library which is injected into running processes (*DG API);*
- the set of eight kernel-mode drivers (*DG Master)*;

- the file scanner used for classification/discovery, (*DG Scanner);*
- and the cryptographic module used for file and removable media encryption, (*VSEC*).

The *DG API* runs silently and is injected into running processes and user mode applications. The *DG Master* drivers are inserted into system stacks (network, print, clipboard, etc.), allowing them to monitor all activity, detect violations and execute actions when a rule is triggered. *DG Scanner* performs periodic scans on local storage volumes to identify and classify sensitive data based on contextual attributes. It is used in conjunction with the AFE to encrypt files matching set criteria.

The *DG Agent* leverages its own instance of the FIPS 140-2 validated VSEC module. Its primary use of cryptography is in the following two components: RME and AFE. Based on contextual rules contained within a security policy, RME and AFE encrypt and decrypt files selectively and automatically, and if configured by policy, without end-user knowledge or action.

The *DG Server* consists of a set of application logic and web services used for managing and transmitting policies to the *DG Agents*, as well as receiving agent "bundles", or collections of forensic activity occurring on the *DG Agent* host systems. It also provides a web-based control center application, known as the *DG Management Console (DGMC)*, which consists of a user interface that TOE administrators interact with to perform management tasks, such as creating and assigning rules and policies, deploying and configuring agents, managing DGMC users and roles, managing alerts, and running activity reports.

1.4.2 TOE Environment

The TOE depends on and integrates with several components in the Operational Environment. The Digital Guardian database server is a separate server-class computer running Microsoft SQL Server, which the *DG Server* uses to store all TSF configuration, including policies, rules, DGMC accounts, events containing real-time and historical forensic information, and a registry of installed *DG Agents*. The DG database server is divided into two databases: Collections and Reporting. Collections stores the daily event information and TSF configuration, while Reporting stores historical data for DG reports.

The TOE integrates with an external LDAP server to provide user account attributes used in authentication, as well as identification of end-users on protected computers. The LDAP server also provides synchronization of computer objects used to manage agent installations. A separate SMTP server also must be installed to provide support for email notifications.

The underlying components necessary for supporting the DG Server include: Microsoft IIS, .NET Framework, and the Windows Server 2008 R2 OS, which contains the Microsoft Server 2008 R2 Cryptographic Primitives Library (BCRYPTPRIMITIVES). IIS is the web server software used to serve the DGMC to end users via a remote web browser. .NET contains the support libraries necessary to run the DG Server application. BCRYPTPRIMITIVES provides cryptographic functionality for securing management traffic between remote administrators and the DGMC, as well as the communication between DG Server and DG Agents.

On DG Agent systems, the TOE Environment consists of Windows XP SP3, Windows 7, Windows Server 2003 SP2/R2, and Windows Server 2008 R2. Cryptographic functionality is implemented the RSAENH or BCRYPTPRIMITIVES modules, depending on the platform.

Figure 3 shows the details of the deployment configuration of the TOE:

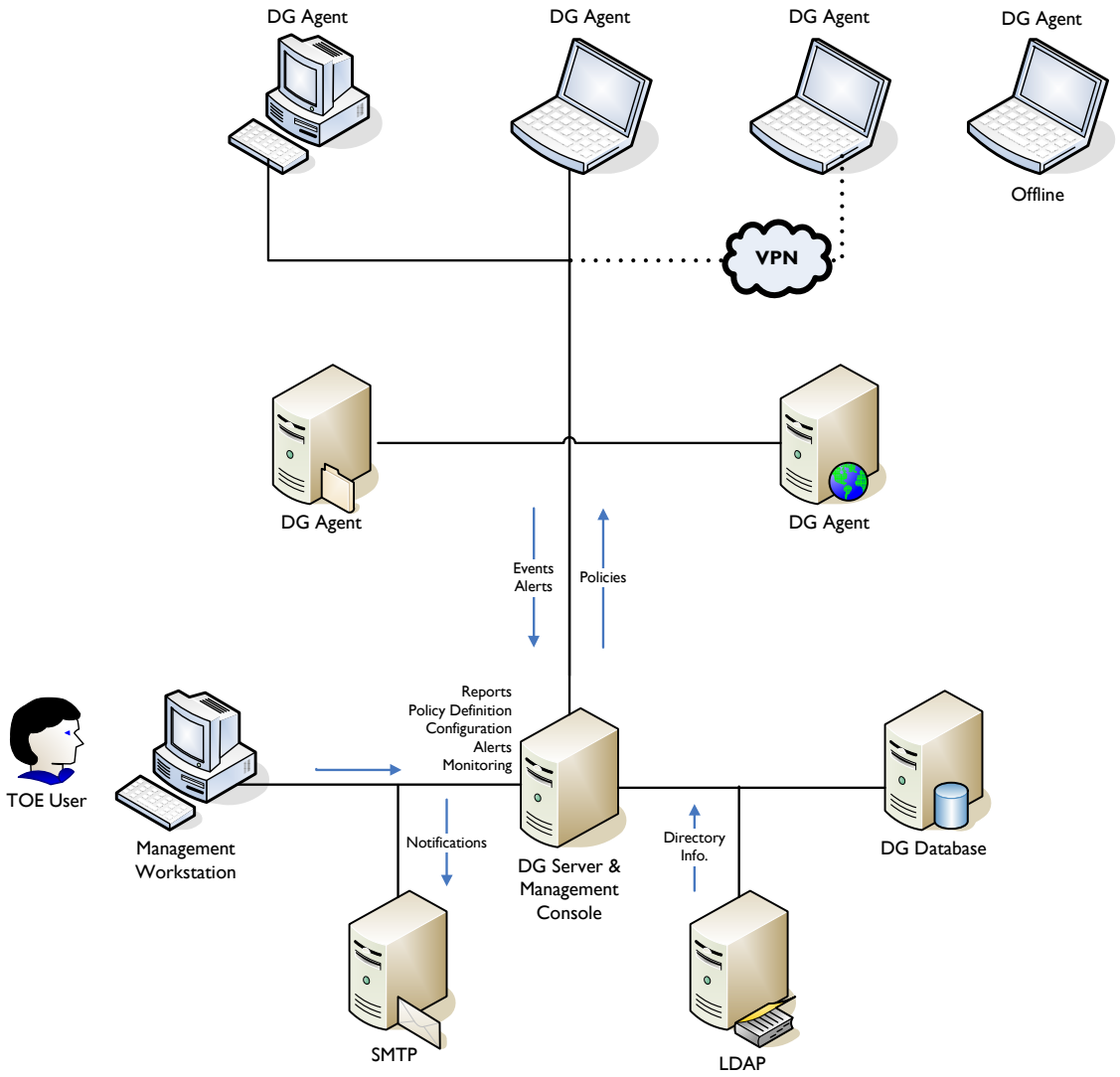

Figure 3 - Deployment Configuration of the TOE

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

Table 2 - TOE Environment Minimum Requirements

Component	Hardware Requirements	Software Requirements
DG Server	Varies depending on the number of monitored nodes; the following specifications are for a single DG Server servicing up to 2500 DG Agents: • 2 x Intel Xeon 3.0 GHz[4] CPU[5] • 4 GB[6] of RAM[7]	• Microsoft Windows Server 2008 R2 SP1 running in single-user mode • bcryptprimitives.dll • Microsoft IIS 7.5 • Microsoft .NET 4.0 • Microsoft ASP.NET enabled

[4] GHz – Gigahertz
[5] CPU – Central Processing Unit
[6] GB – Gigabyte

Component	Hardware Requirements	Software Requirements
	• 73 GB RAID 1[8] storage • Gigabit network adapter	• Valid TLS[9] certificate in .pfx format • FIPS mode enabled[10]

DG Agent	• Pentium 4 CPU
	• 512 MB[11] of RAM
	• 200MB+ on fixed disk
		• **Operating Systems**
		  • Windows XP SP3 (32 and 64-bit)
		  • Windows Server 2003 SP2/R2 (32 and 64-bit)
		  • Windows 7 SP1 (32 and 64-bit)
		  • Windows Server 2008 R2 SP1 (64-bit)
		• RSAENH.dll or bcryptprimitives.dll
		• FIPS mode enabled

DG Management Console	• 1024x768 monitor resolution	• Internet Explorer 7.0 or higher
DG Database	Varies depending on configuration; the following specifications are for a single database server supporting a 2500 agent DG Server: • 2 x Intel Xeon 3.0 GHz CPU • 4 GB of RAM • 73 GB RAID 1 storage • Gigabit network adapter	• Microsoft Windows Server 2008 R2 SP1 • Microsoft SQL Server 2008 Standard R2 SP1
LDAP Server	Varies depending on configuration	• Microsoft Windows Server 2008 Active Directory
SMTP Server	Varies depending on configuration	• SMTP mail server for Alerts and Email Notifications

1.5 TOE Description

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

1.5.1 Physical Scope

The TOE is a set of software-based client and server applications which run on the Windows OS installed on server- and workstation-class hardware compliant to the minimum requirements as listed in Table 2. The client components of the TOE (*DG Agents)* are installed on all enterprise desktops, laptops, and servers intended to be protected by the TOE, and the server component (*DG Server*) is installed on centralized servers located in a data center with network accessibility to all *DG Agents*, as depicted in Figure 3 above. In this scenario, some *DG Agent* computers are directly connected to the enterprise network, and others through a Virtual Private Network (VPN) or in an offline state. The *DG Management Console* is accessed through a separate management workstation using a standardized web browser.

[7] RAM – Random Access Memory
[8] RAID 1 – Redudant Array of Independent Disks Level 1 Mirroring
[9] TLS – Transport Layer Security
[10] On Microsoft Windows XP and later versions, the setting "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" must be enabled to support FIPS mode of operation.
[11] MB – Megabyte

The TOE boundary includes the Digital Guardian application server software, the core DG Windows Agent, and the AFE and RME modules, but should exclude the remaining add-on modules, Linux agents, Networking Agent (Fidelis Appliance), eDiscovery Agent, IIS, .NET Framework, BCRYPTPRIMITIVES, RSAENH, underlying OS, database servers, and hardware/virtual hypervisors.

In the CC-evaluated configuration, the TOE is installed on a minimum of five computers. The following list encompasses the physical or virtual components necessary for supporting the TOE:

- Windows 2008 R2 based Digital Guardian Server computer
- Windows XP SP3 or Server 2003 SP2/R2 (32-bit) based Digital Guardian Agent computer
- Windows XP SP3 or Server 2003 SP2/R2 (64-bit) based Digital Guardian Agent computer
- Windows 7 (32-bit) based Digital Guardian Agent computer
- Windows 7, or 2008 R2 (64-bit) based Digital Guardian Agent computer

The following physical/virtual components do not contain any functionality included within the TOE boundary; however, they are either necessary for full enforcement of the TSF, or integrate with the TOE to provide additional functionality to support TSF-related services:

- Microsoft SQL Server based Digital Guardian Database Server computer (required for storing the DG Database and audit logs)
- SMTP server computer (required for sending alert notification emails)
- LDAP server computer (required for synchronizing user attribute data for identification and authentication, and computer object information for deployment and DG Agent management functions)

Figure 4 depicts the physical TOE boundary and included components, as well as components excluded from the boundary. Also shown are the cryptographic boundaries for the VSEC module, and any 3rd party cryptographic providers implemented by the TOE.

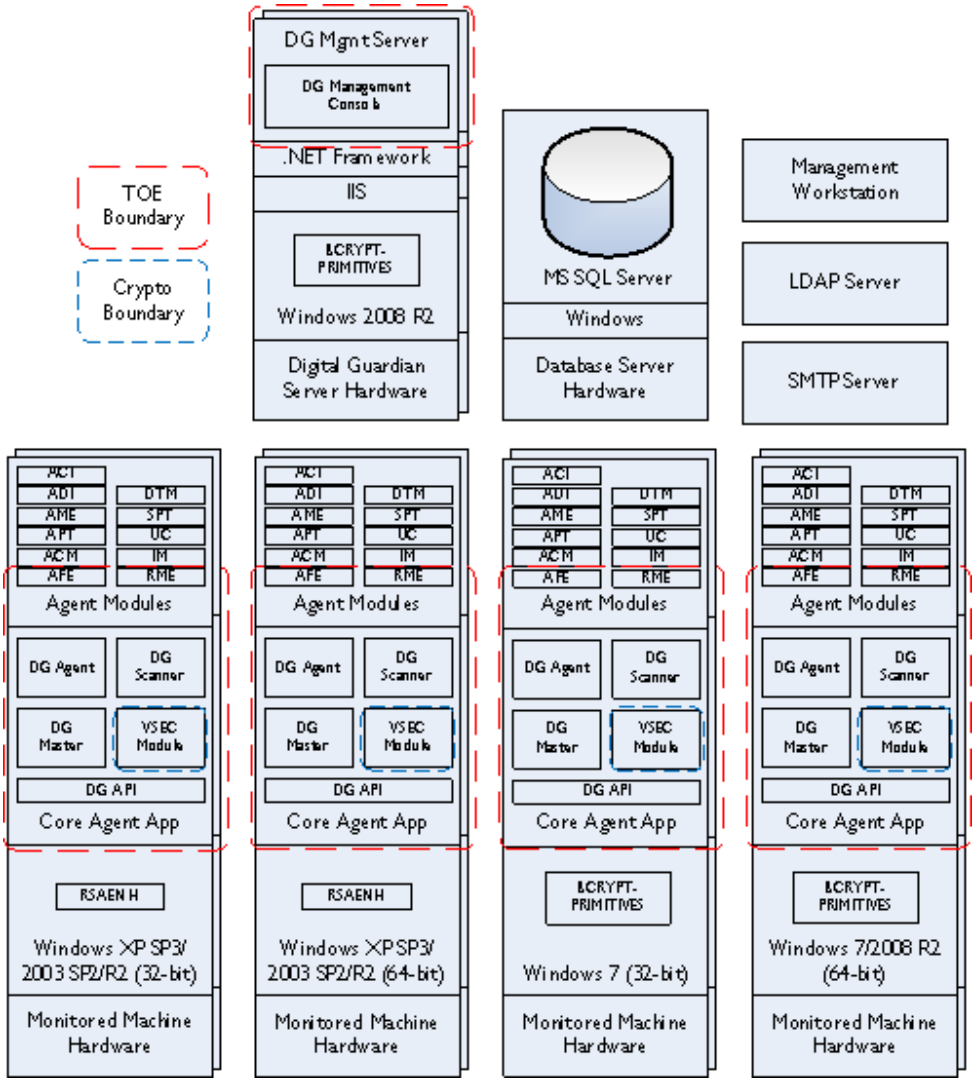

Figure 4 - Physical TOE Boundary

1.5.1.1 TOE Software

The server component is a web-based application server written in C#.NET designed to run on the Microsoft .NET framework on customer-owned hardware running Windows Sever 2008 R2 and IIS 7.5. The application server functions as both a management console and a communications hub to the deployed agent software. The server component is expected to be installed on a system compliant to the minimum software and hardware requirements as listed in Table 2.

The application server relies on Microsoft SQL Server to store its various databases. The SQL Server software and databases are installed on separate hardware from the application server. Configuration of the SQL Server and .NET application server is normally conducted by Verdasys Professional Services personnel.

The core of the Digital Guardian Windows agent is a set of flexible kernel-level processes that hide themselves from the rest of the OS and "own" everything in the system. This allows the agent to monitor and control practically everything that happens in the system. Digital Guardian includes eight different

system drivers that allow the product to inject itself into and control every system stack (network, print, clipboard, etc.).

The agent is written in C/C++, and is modular in design. Its core components include *DG Agent*, which communicates with the applications server and manages policies in the local agent database, *DG API*, which is injected into running processes, *DG Scanner*, which performs discovery on behalf of the agent modules, *DG Master*, which runs in the kernel space, and the VSEC FIPS module. VSEC is a software module that provides cryptographic functionality for Digital Guardian's RME and AFE modules, and other Verdasys add-on components. Within the Digital Guardian architecture, it resides only on the *DG Agent* computers.

The agent software is identical, at the source code level, for each instance of the DG Agent build on the following supported OS platforms and architectures:

- Windows XP SP3 and Server 2003 SP2/R2 (32-bit)
- Windows XP SP3 and Server 2003 SP2/R2 (64-bit)
- Windows 7 (32-bit)
- Windows 7 and Server 2008 R2 (64-bit)

1.5.1.2 Guidance Documentation

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

- *Digital Guardian Rule Implementation Guide*
- *Digital Guardian Server Minimum Requirements*
- *Digital Guardian Unattended Deployment Guide*
- *Digital Guardian Utilities*
- *Installing and Upgrading Digital Guardian*
- *Installing and Using Digital Guardian Archive and Restore for SQL Server*
- *Quick Reference Verdasys Digital Guardian*
- *Release Notes: Digital Guardian*
- *Using Digital Guardian*
- *What's New: Digital Guardian*

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security functions, which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are as follows:

- Robust Security Management
- Enterprise Information Protection
- Cryptographic Protection
- Violation Analysis, Alerting, and Reporting
- Fault Tolerance

1.5.2.1 Robust Security Management

The DG Server implements the Management Access Control Security Function Policy (SFP), which ensures that DGMC Users are appropriately identified, authenticated, and authorized for managing the TOE. It also defines the security attributes used to determine the actions allowable for DGMC Users, and the authorized roles which are permitted to define security attributes. In addition, it restricts attribute values to restrictive or permissive defaults, where appropriate. Security attributes used to enforce the Management Access Control SFP include: user IDs[12], passwords, roles, role privilege levels, policy rules, rule properties, and alert subscriptions.

[12] ID - Identification

The DG Server enforces identification and authentication for users of the DGMC. Subjects are required to enter a valid username, password, and domain prior to being presented with DGMC user interface elements. No anonymous access is provided. Interface elements displayed to the user are based on the user's authorized roles/privilege levels, which are discussed in section 7.1.1.

The DG Server provides several management functions to authorized DGMC Users and Administrators, including user/role management, DG Agent configuration, rule and policy management, alert management, and reporting. The Management Access Control SFP is enforced to ensure that only users with the authorized roles can perform administrative functions. All activity performed through the DGMC is recorded by the DG Server, such as policy changes, agent configuration changes, etc. Audit records are viewable by the System Adminstrator.

The DGMC is accessible using a web browser installed on the management workstation over HTTPS. The DGMC implements robust session security for users of the DGMC by displaying an access banner prior to authentication, and automatically terminating sessions after a configurable time period.

The DG Agent has two options for providing tamper protection: Stealth mode and Tamper Resistance mode. Stealth mode effectively makes all DG processes and configuration files and registry entries invisible, while Tamper Resistance mode protects DG processes, registry entries, files, and services from modification or termination by unauthorized personnel, including system administrators. The Management Access Control SFP ensures that the end-users are prevented from observing or disabling the DG-related processes and configuration. DG Agents can only be disabled or uninstalled by Administrators who possess a shared secret that is established during the TOE installation process.

1.5.2.2 Enterprise Information Protection

The DG Agents enforce the Enterprise Information Protection SFP for users of the TSF-mediated workstations and servers using a set of rules as defined within a policy associated with the machine or user on which the DG Agent is installed. The TOE is capable of monitoring and controlling virtually all OS actions involving data, including, but not limited to: mediating or filtering copy/paste operations, preventing legacy or unapproved applications from running, burning to CD/DVD, sending sensitive email attachments, deleting or copying files, uploading files to network locations, and printing. For example, within the file system, the DG Agent can monitor and block file read, write, open, move, copy, rename, delete, recycle, and restore operations. It can also monitor and control network downloads, perform screen captures, control USB device attachment, and mediate access to remote drives.

DG Agents enforce several types of rules, including:

- Application Management Rules
- Control Rules
- Classification Rules
- Filter Rules
- Trusted Process Rules
- Data Vault Rules
- Component Rules

DG rules are consolidated into policies which are applied to users or computers, and are categorized as follows:

- Control Policies
- Classification Policies
- Filter Policies
- Trusted Process Policies

The rules and policies listed above are described in greater detail in section 7.1.2.

DG Agents communicate regularly with the DG Server to retrieve up-to-date policies, ensuring that the most current policies are immediately and continuously enforced on monitored systems in the TOE environment. In addition, the DG Agent uploads activity bundles containing events and alerts to the DG Server, where they can be processed and analyzed by TOE administrators, or sent as email alert notifications.
To protect transmitted bundle data from disclosure, the VSEC module generates symmetric AES[13]-256 session keys, which are used to encrypt bundles. The symmetric keys are wrapped using asymmetric RSA[14]-2048 keys, which are generated and imported from the TOE environment. The DG Agent also signs bundle data to ensure its authenticity.

Typically, the DG Agent examines files in motion or in use, however, it does not process files that the user is not interacting with. For features like AFE, the DG Scanner is used to actively scan the contents of the local hard drive to encrypt files based on Classification and Control Rules. Classification rules are used to identify sensitive data based on contextual object attributes, such as file extensions, file locations, process names, etc., which are maintained in the local agent database and are used to trigger encryption or other actions specified within the Control rules. The DG Scanner can be configured to run at an interval to ensure timely protection of newly created sensitive data.

1.5.2.3 Cryptographic Protection

The FIPS 140-2 validated VSEC module provides symmetric key generation, symmetric encryption and decryption, key transport, digital signatures, cryptographic hashing, and hash based message authentication (HMAC) functions using approved ciphers and key sizes, in accordance with approved government standards. Symmetric keys are generated using an approved deterministic random bit generator (DRBG) and are zeroized from memory buffers according to FIPS requirements. Asymmetric keys are imported from an existing public key infrastructure (PKI) via an API call. The VSEC module is utilized to provide cryptographic operations requested by the AFE and RME modules, and to protect bundle data from disclosure while transmitted to the DG Server.

The full list of ciphers/key lengths implemented by the VSEC module is described in section 7.1.3.

The VSEC module is identical, at the source code level, for the following supported OS platforms:

- Windows XP SP3, 32-bit and 64-bit
- Windows 7, 32-bit and 64-bit
- Windows Server 2003 SP2/R2, 32-bit and 64-bit
- Windows Server 2008 R2, 64-bit

Validation compliance for the VSEC module is maintained for the above vendor-affirmed platforms per the cryptographic porting requirements found in the *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*, G.5, "Maintaining Validation Compliance of Software or Firmware Cryptographic Modules".

1.5.2.4 Violation Analysis, Alerting, and Reporting

The DG Agent generates events for all types of actions that the TOE is capable of monitoring, such as file operations (move, delete, burn to DVD, etc.) or application operations (copy/paste, launch executable, etc.). These events are assembled into collections, known as bundles, and sent to the DG Server to be recorded into the Collection database. Rules which govern the behavior of users and applications have the option of

[13] AES – Advanced Encryption Standard
[14] RSA – Rivest, Shamir, Adleman

generating an alert when a particular event threshold is met or if a rule is violated. When these types of rules are triggered, an alert notification is sent via SMTP to a DGMC User who has subscribed to that alert.

Each notification provides the recipient with information on the alert, error condition, or failure, which contains the necessary details to aid in an investigation of the root issue. Each Control Rule has an associated severity level, which determines the risk associated with a violation of the rule. Users can choose to subscribe to alert notifications based on the assigned severity levels.

Using the Reporting feature, authorized DGMC Users run reports detailing events based on several factors, including users, time period, or severity level. Alerts generated by a triggered rule are analyzed by an Alert Manager and resolved to remove them from the list of alerts. Alert investigators assign resolution codes to indicate that the alert was analyzed and processed.

1.5.2.5 Fault Tolerance

In the event of a communications outage, the DG Agent continues to enforce the most recently downloaded policies, and, upon re-establishment of communication, will immediately download and apply any policies created or updated during the outage. While the outage is in effect, the DG Agent preserves forensic activity bundles and attempts to retransmit the data until the DG Server is once again accessible. In the event that the DG Server is unable to write to the database, the DG Server generates an error in the Windows event log.

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

The Product Features/Functionality that are not part of the TOE are:

- RME Private Encryption
- DG Agent Modules
  - Adaptive Mail Encryption
  - Adaptive Content Inspection
  - Adaptive Data Inspection
  - Advanced Persistent Threat
  - Application Compliance
  - Documentum Extension
  - SharePoint Extension
  - User Classification
  - Investigation Module
- Blackberry Enterprise Server Agent
- Citrix/Terminal Server Agent
- DG Agent for Linux
- eDiscovery Agent
- Exchange ActiveSync
- Fidelis Appliance/DG Network Agent
- Manual/Corporate Uninstall Key

1.5.4 FIPS 140-2 Considerations for the TOE Environment

To protect the the information transmitted between separate parts of the TOE, The DG Server and Agent implement functionality which relies on cryptographic providers in the TOE Environment.

On the DG Server, the DGMC web application is secured using HTTPS. In addition, the DG Agent and Server communicate using a web service which is also secured with HTTPS. In the evaluated

configuration, TLS support is implemented through the underlying IIS web server. Cryptographic functionality for the DG Server is provided by the FIPS 140-2 validated Microsoft Windows 2008 R2 Cryptographic Primitives Library (BCRYPTPRIMITIVES), for the use in the following operations: asymmetric/symmetric key generation, encryption/decryption, hashing, digital signature generation and verification, and keyed hash message authentication. During installation, a PKCS#12 certificate containing a private and public key pair must be imported from an existing PKI.

The DG Agent implements cryptographic functionality to support TLS, which is provided by various FIPS 140-2 validated modules depending on the platform: the BCRYPTPRIMITIVES module on Windows 7 and Server 2008 R2, or the Microsoft Windows Enhanced Cryptographic Provider (RSAENH) on Windows XP SP3 and Server 2003 SP2/R2. These modules are used in the following operations: asymmetric key generation and exchange, encryption/decryption, and message authentication for TLS.

In the evaluated deployment configuration, the Microsoft Windows 2008 R2 OS underlying the DG Server, as well as the Windows XP SP3, 7, Server 2003 SP2/R2, and Server 2008 R2 OS underlying the DG Agent operate in single-user mode with the FIPS mode Group Policy option set to enabled.

For more information on the Microsoft cryptographic providers in the TOE Environment, please refer to the following:

- *Microsoft Windows Server 2008 R2 Cryptographic Primitives Library (bcryptprimitives.dll) FIPS 140-2 Security Policy* (Certificate #1336).
- *Microsoft Windows 7 Cryptographic Primitives Library (bcryptprimitives.dll) FIPS 140-2 Security Policy* (Certificate #1329)
- *Microsoft Windows Server 2003 Enhanced Cryptographic Provider (RSAENH) FIPS 140-2 Security Policy* (Certificate #1012)
- *Microsoft Windows XP Enhanced Cryptographic Provider (RSAENH) FIPS 140-2 Security Policy* (Certificate #989

2 Conformance Claims

This section and Table 3 provide the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 3 - CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the Common Evaluation Methodology (CEM) as of 2011/08/04 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ Augmented with Flaw Remediation (ALC_FLR.2)

3 Security Problem

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

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

3.1 Threats to Security

This section identifies the threats to the IT[15] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into three categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)
- End-users of TOE-protected resources: They have little to no knowledge of the TOE, however may possess the privileges necessary to access and modify sensitive data within an organization, and may either knowingly or unknowingly disclose such information. End-users who pose a threat are assumed to be either malicious, or non-malicious but careless or otherwise ignorant to the organization's security policy. Note that end-users are assumed to have non-administrative privieleges, and cannot perform activities such as installing software applications, setting system time, etc.

Attackers and TOE users are assumed to have a low level of motivation, while end-users may have a high level of motivation, but a low skill level. The IT assets requiring protection are the TSF[16] and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 4 below lists the applicable threats.

Table 4 - Threats

Name	Description
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security enforcement mechanisms.
T.DISABLE	A malicious or careless user may suspend or terminate the TOE agent's operation, rendering its ability to mediate access control upon the TOE environment or protected data useless.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to the TOE server.
T.FALSIFY	A malicious user can falsify the identity of a TOE agent, providing the administrator with false assurance that the TOE is enforcing a policy.

[15] IT – Information Technology
[16] TSF – TOE Security Functionality

Name	Description
T.FORGE	A malicious user may create a false policy and send it to the TOE agent for consumption, adversely affecting its access control policy enforcement behavior.
T.UNATTEND	A TOE server administrator may leave an authenticated session unattended, resulting in the possibility of a malicious or unauthorized user to mask their actions as the logged in user, resulting in a misconfiguration or alteration of the TSF behavior.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.NODETECT	An administrative user or end-user's actions may go undetected or be incorrectly recorded, resulting in a failure to identify a potential security breach.
T.NOROUTE	A malicious user may disrupt the internal communications between TOE server and TOE agent, adversely affecting access control behavior.
T.TAMPERING	A user or process may be able to bypass the TOE agent's security mechanisms by tampering with the TOE server, TOE agent, or TOE environment.
T.UNAUTH	A user may bypass the TOE server's identification, authentication, or authorization mechanisms in order to illicitly utilize the TOE's management functions.
T.UNAUTH2	A malicious or careless user may access an object in the TOE environment that causes disclosure of sensitive or proprietary data, or adversely affects the behavior of a system.
T.WEAKPOL	A policy administrator may be incapable of using the TOE server to define policies in sufficient detail to facilitate robust access control, causing the TOE agent's access control mechanism to behave in a manner that allows illegitimate activity or prohibits legitimate activity.
T.UNOBSERV	A malicious or careless end-user may instigate a high-risk security event or policy, which may go unnoticed by the TOE operators responsible for enforcing the organizational security policy.
T.WEAKCIPHERS	A TOE administrator may improperly configure the TOE to use weak ciphers and key sizes, thus compromising the TOE's ability to protect user data.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. Table 5 below lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration.

Table 5 - Organizational Security Policies

Name	Description
P.MANAGE	The TOE server and TOE agent may only be managed by authorized

Name	Description
	users.
P.INTEGRITY	Data collected and produced by the TOE server and TOE agents must be protected from modification.
P.BANNER	The TOE server shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
P.UPDATEPOL	The organization will exercise due diligence to ensure that the TOE is updated with relevant policy data.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 6 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 6 - Assumptions

Name	Description
A.AUTHENTICATE	Subjects acting as end-users of the TOE agent are authenticated by a secure mechanism in the TOE environment that works in conjunction with the repository responsible for maintaining user identity and attribute data.
A.ENDUSERS	End-users of the TOE are assumed to posess a low-skill level with little to no knowledge of the TOE, and are not afforded local administrator rights on TOE agent-mediated machines.
A.INSTALL	The TOE is installed on the appropriate, dedicated hardware and operating system necessary to support the error-free operation of the TSF.
A.LOCATE	The TOE server is located within a controlled access facility.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NETCON	The TOE environment provides the network connectivity required to allow distributed TOE components to communicate.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.SECURECOMM	Because the TOE's distributed components (server and agent) may not be located within the same controlled access facility or connected to the same protected physical network, it is assumed that the IT environment will provide a secure line of communication between the TOE server and agent and between the TOE server and remote administrators.
A.TIMESTAMP	The IT environment provides the TOE server and TOE agent with the necessary reliable timestamps.

Name	Description
A.USERID	Identity and attribute data for TOE agent users is provided by a secure organizational repository in the TOE environment.

4 Security Objectives

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

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 7 below.

Table 7 - Security Objectives for the TOE

Name	Description
O.ADMIN	The TOE server and TOE agent must include a set of functions that allow efficient management of their functions and data, ensuring that TOE users with the appropriate privileges and/or secrets, and only those TOE users, may exercise such control.
O.AUDIT	The TOE agent will provide measures for generating security relevant events upon detecting access attempts to TSF-mediated resources in the TOE Environment, and the TOE server provides a mechanism through which the events can be reviewed by authorized administrators. The TOE server must also record events for operations performed through its management interfaces, as well as any relevant details, including outcome.
O.AUTH	The TOE server will provide a mechanism to examine user identity and credential data supplied by a user and compare it with the information stored in its database to determine the extent to which the claimed identity should be able to perform TSF management functions.
O.BANNER	The TOE server will display an advisory warning regarding use of the TOE.
O.DATAPROT	The TOE agent will protect sensitive user data from unauthorized access, modification, loss, or disclosure by enforcing an access control policy produced by the TOE server, and by performing classification and encryption of data according to a set of sensitivity criteria. The TOE server must ensure that only authorized administrators possess the ability to configure policies to be enforced by the TOE agent.
O.DISTRIB	The TOE server will provide the ability to manage the behavior of TOE agents using secure channels.
O.EAVES	The TOE agent will leverage a FIPS 140-2 validated cryptographic module to secure the communication channels to and from itself.
O.INACTIVE	The TOE server must implement a robust mechanism for terminating user sessions after a period of inactivity.
O.MAINTAIN	The TOE agent will be capable of maintaining policy enforcement even if disconnected from the TOE server.
O.MONITOR	The TOE server and TOE agents will monitor the behavior of themselves for anomalous activity.

Name	Description
O.NOTIFY	The TOE server must possess the capability of detecting policy violations and alerting the appropriate personnel when such anomalous activity occurs.
O.POLICY	The TOE server will provide capabilities for managing policies that the TOE agents will enforce, based on a set of rules containing subject and object attributes.
O.PROTECT	The TOE server must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.
O.RESILIENT	The TOE agent must prevent users in the Operational Environment from performing actions that would disable or otherwise modify its behavior.
O.STRONGCRYPTO	The TOE agent must implement a FIPS 140-2 validated cryptographic module leveraging secure approved algorithms to protect sensitive data and CSPs from modification or disclosure.
O.REVIEW	The TOE server must provide a mechanism to identify access control policy violations and to provide tools necessary to view and respond to violations by authorized TOE operators.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 8 below lists the IT security objectives that are to be satisfied by the environment.

Table 8 - IT Security Objectives

Name	Description
OE.ADMIN	There will be one or more administrators of the TOE environment that will be responsible for providing subject identity to attribute mappings within the TOE.
OE.CRYPTO	The TOE environment must be able to provide FIPS 140-2 validated cryptography to protect communications between the TOE server and TOE agent over insecure networks.
OE.ENDUSERS	The TOE environment shall restrict end-users of the TSF-mediated workstations to limited or non-administrative privileges.
OE.NETWORK	The TOE environment must consist of a dedicated, secure network, to which distributed TOE components will be attached, along with other services necessary to support the TSF, such as a central repository for supplying user and computer identity information.
OE.PLATFORM	The TOE hardware and OS must support all required TOE functions.

Name	Description
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering. To ensure this, operating systems on which the TOE software is installed must be appropriately secured following best practices guidance, and that all high-level security risks have been mitigated. This might include installing anti-virus software on the operating systems which support the TOE, as well as placement of firewalls and intrusion detection sensors in the appropriate network locations.
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.
OE.USERID	The TOE environment must be able to identify the user requesting access to TSF-mediated resources and convey validation of this to the TOE.

4.2.2 Non-IT Security Objectives

Table 9 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 9 - Non-IT Security Objectives

Name	Description
NOE.MANAGE	Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.
NOE.PHYSICAL	The physical TOE server environment must be suitable for supporting a computing device in a secure setting and must provide adequate physical security to prevent unauthorized access or tampering.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 10 identifies all extended SFRs implemented by the TOE

Table 10 - Extended TOE Security Functional Requirements

Name	Description
ESM_ACD_EXT.1	Access Control Policy Definition
ESM_ACT_EXT.1	Access Control Policy Transmission
ESM_DSC_EXT.1	Object Discovery
ESM_OAD_EXT.1	Object Attribute Definition

5.1.1 Class ESM: Enterprise Security Management

Enterprise security management (ESM) functional requirements pertain to behaviors that support the centralized management of authentication, authorization, accountability, and compliance activities in an organization. This class specifies functional activities that support class FDP and FIA by requiring the TSF to provide data that is used for data protection and authentication activities. The CC family FDP_ACC: Subset Access Control was used as a model for the extended family ESM_ACD_EXT: Access Control Policy Definition. The family FDP_IFF: Information Flow Control Functions was used as a model for the extended family ESM_ACT_EXT: Access Control Policy Transmission. The family FAU_ARP: Audit Automatic Response was used as a model for the extended family ESM_DSC_EXT: Object Inventory. The CC families FIA_ATD: User Attribute Definition and FIA_USB: User Subject Binding were used as models for the extended family ESM_OAD_EXT: Object Attribute Definition.

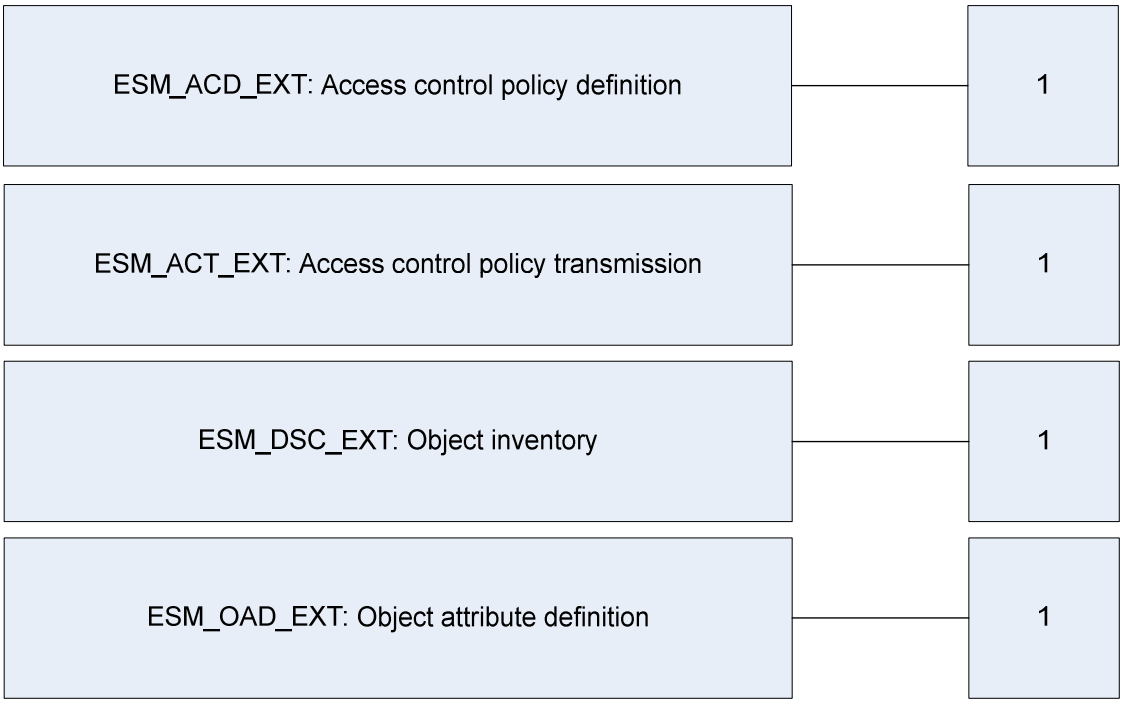

Figure 5 - ESM: Enterprise Security Management Class Extended Family Decomposition

5.1.1.1 Access control policy definition (ESM_ACD_EXT)

Family Behavior

The requirements of this family ensure that the TSF will have the ability to authoritatively define access control policies for use in an ESM deployment. The ESM_ACD_EXT family defines requirements for defining access control policies. The ESM_ACD_EXT.1 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to define policies which govern the behavior of other distributed TOE components.

Component Leveling

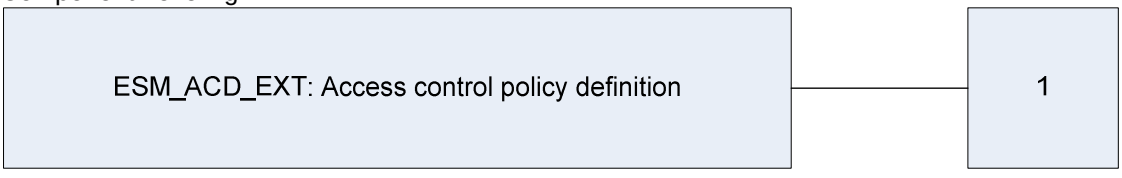

Figure 6 - ESM_ACD_EXT: Access Control Policy Definition family decomposition

ESM_ACD_EXT.1, access control policy definition, requires the TSF to be able to define access control policies for consumption by internal access control agents.

Management: ESM_ACD_EXT.1

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

- Creation and modification of policies.

Audit: ESM_ACD_EXT.1

The following actions should be auditable if ESM_ACD_EXT.1 Access control policy definition is included in the PP/ST:

- Minimal: Creation and modification of policies.

ESM_ACD_EXT.1 Access control policy definition
Hierarchical to: No other components
ESM_ACD_EXT.1.1

The TSF shall provide the ability to define access control policies for consumption by one or more Access Control agents.

ESM_ACD_EXT.1.2

Access control policies defined by the TSF must be capable of containing the following:

a) Subjects: [***assignment: list of subjects that can be used to make an access control decision and the source from which they are derived***]; and
b) Objects: [***assignment: list of objects that can be used to make an access control decision and the source from which they are derived***]; and
c) Operations: [***assignment: list of operations that can be used to make an access control decision and the source from which they are derived***]; and
d) Attributes: [***assignment: list of attributes that can be used to make an access control decision and the source from which they are derived***].

ESM_ACD_EXT.1.3

The TSF shall associate unique identifying information with each policy.

Dependencies: No dependencies

5.1.1.2 Access control policy transmission (ESM_ACT_EXT)

Family Behavior

The requirements of this family ensure that the TSF will have the ability to transfer defined access control policies to other TOE components. The ESM_ACT_EXT family defines requirements for transmitting policy data to authorized entities. The ESM_ACT_EXT.1 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to distribute access control policy data to distributed TOE components.

Component Leveling

Figure 7 - ESM_ACT_EXT: Access Control Policy Transmission family decomposition

ESM_ACT_EXT.1, access control policy transmission, requires the TOE to transmit access control policy data defined by ESM_ACD_EXT.1 to compatible and authorized TOE agents under conditions defined by the ST author.

Management: ESM_ACT_EXT.1

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

- Specification of the access control policy data to be transmitted.
- Specification of the circumstances under which this data is transmitted.
- Specification of the destinations to which this data is transmitted.

Audit: ESM_ACT_EXT.1

The following actions should be auditable if ESM_ACD_EXT.1 Access control policy transmission is included in the PP/ST:

- Minimal: Transmission of access control policy data to authorized access control agents.

ESM_ACT_EXT.1 Access control policy transmission
Hierarchical to: No other components
ESM_ACT_EXT.1.1

The TSF shall transmit policies to compatible and authorized Access Control agents under the following circumstances: [selection: choose one or more of: immediately following creation of a new or updated policy, at a periodic interval, at the request of a compatible Secure Configuration Management product, [*assignment: other circumstances*].

Dependencies: ESM_ACD.1 Access control policy definition

5.1.1.3 Object inventory (ESM_DSC_EXT)

Family Behavior

The requirements of this family ensure that the TSF will have the ability to identify Operational Environment objects and take some action based on this identification. The ESM_DSC_EXT family defines requirements for taking an inventory of objects in the Operational Environment that exhibit certain characteristics and acting upon those objects in some manner. This pertains to enterprise security management because the ability of the TSF to perform this action supports the primary function of an enterprise security management TOE (in this case, access control). The ESM_DSC_EXT.1 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to examine and act upon an observation made of the Operational Environment.

Component Leveling

Figure 8 - ESM_DSC_EXT: Object Inventory family decomposition

ESM_DSC.1_EXT, object discovery, requires the TSF to search the Operational Environment for data that meets some criteria and take action based upon discovery of such data. The primary purpose of this requirement is for use in mandatory access control (MAC) or similar environments so that the TSF can identify data that is not in a location allowed by its associated attributes and subsequently take some form of corrective action based on this.

Management: ESM_DSC_EXT.1

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

- Specification of detection criteria.
- Specification of actions taken upon discovery of object which meet detection criteria.

Audit: ESM_DSC_EXT.1

The following actions should be auditable if ESM_DSC_EXT.1 Object discovery is included in the PP/ST:

- Minimal: Discovery of objects which meet detection criteria.
- Minimal: Action taken against discovered object

ESM_DSC_EXT.1 Object discovery
Hierarchical to: No other components
ESM_DSC_EXT.1.1
The TSF shall be able to discover objects in the Operational Environment which meet the following conditions: [selection: unencrypted data which policy requires to be encrypted, data which resides in a domain that is inconsistent with the data's defined sensitivity attributes, [***assignment: other condition which indicates that data which resides in the Operational Environment should be catalogued by the TSF***]].
ESM_DSC_EXT.1.2
The TSF shall take the following actions upon discovery of an object as defined by ESM_DSC.1.1: [selection: encrypt the object, move the object to a location consistent with its sensitivity attributes, delete the object, [***assignment: other action***]].
Dependencies: No dependencies

5.1.1.4 Object attribute definition (ESM_OAD_EXT)

Family Behavior
The requirements of this family ensure that the TSF will have the ability to authoritatively define attributes for Operational Environment attributes that can subsequently be used for access control policy definition and enforcement. The ESM_OAD_EXT family defines requirements for specification of object attributes. This allows other ESM products to enforce their own security functions by utilizing attribute data defined by the TSF. The ESM_OAD.1 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to define attributes that are associated with objects that reside in the Operational Environment.

Component Leveling

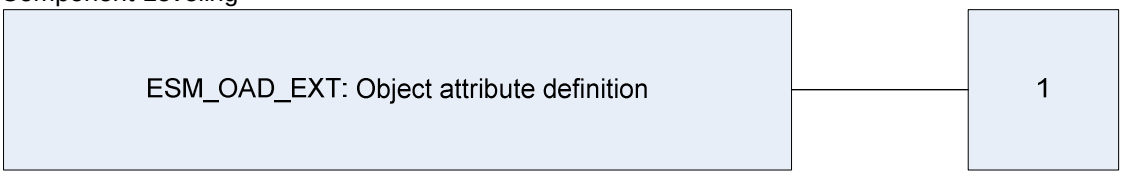

Figure 9 - ESM_OAD_EXT: Object Attribute Definition family decomposition

ESM_OAD_EXT.1, object attribute definition, requires the TSF to be able to define some set of object attributes. These attributes are expected to be subsequently associated with objects in the Operational Environment for use in handling access control. Examples of object attributes include security labels for use in mandatory access control (MAC) environments and protection levels that can be associated with web pages that reside within an organization's intranet.

Management: ESM_OAD_EXT.1
The following actions could be considered for the management functions in FMT:
- Definition of object attributes
- Association of attributes with objects

Audit: ESM_OAD_EXT.1
The following actions should be auditable if ESM_OAD_EXT.1 Object attribute definition is included in the PP/ST:
- Minimal: Definition of object attributes.
- Minimal: Association of attributes with objects

ESM_OAD_EXT.1 Object discovery
Hierarchical to: No other components
ESM_OAD_EXT.1.1
The TSF shall maintain the following list of security attributes belonging to individual objects: [assignment: *list* ***of security attributes***].

ESM_OAD_EXT.1.2

The TSF shall be able to associate security attributes with individual objects.

Dependencies: **No dependencies**

5.2 Extended TOE Security Assurance Components

There are no extended SARs implemented by the TOE.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

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

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

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified appending "_EXT" at the end of the short name.
- Iterations are identified by appending a number in parentheses following the component title. For example, FAU_GEN.1(1) Audit Data Generation would be the first iteration and FAU_GEN.1(2) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 11 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 11 - TOE Security Functional Requirements

Name	*Description*	*S*	*A*	*R*	*I*
ESM_ACD_EXT.1	*Access control policy definition*		✓		
ESM_ACT_EXT.1	*Access control policy transmission*	✓	✓		
ESM_DSC_EXT.1	*Object discovery*	✓	✓		
ESM_OAD_EXT.1	*Object attribute definition*		✓		
FAU_ARP.1	*Security alarms*		✓		
FAU_GEN.1(1)	*Audit data generation (TOE server)*	✓	✓	✓	✓
FAU_GEN.1(2)	*Audit data generation (TOE agent)*	✓	✓		✓
FAU_SAA.1	*Potential violation analysis*		✓		
FAU_SAR.1(1)	*Audit review (TOE server data)*		✓		✓
FAU_SAR.1(2)	*Audit review (TOE agent data)*		✓		✓
FCS_CKM.1	*Cryptographic key generation*				
FCS_CKM.4	*Cryptographic key destruction*		✓		
FCS_COP.1	*Cryptographic operation*		✓	✓	

Name	Description	S	A	R	I
FDP_ACC.1(1)	Subset access control (TOE server)		✓		✓
FDP_ACC.1(2)	Subset access control (TOE agent)		✓		✓
FDP_ACF.1(1)	Security attribute based access control (TOE server)		✓		✓
FDP_ACF.1(2)	Security attribute based access control (TOE agent)		✓		✓
FDP_ITC.1	Import of user data without security attributes		✓	✓	
FIA_UAU.2	User authentication before any action				
FIA_UID.2	User identification before any action				
FMT_MOF.1	Management of security functions behaviour	✓	✓	✓	
FMT_MSA.1	Management of security attributes	✓	✓	✓	
FMT_MSA.3	Static attribute initialisation	✓	✓	✓	
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_FLS.1	Failure with preservation of secure state		✓		
FRU_FLT.1	Degraded fault tolerance		✓		
FTA_SSL.3	TSF-initiated termination		✓		
FTA_TAB.1	Default TOE access banners				
FPT_ITT.1	Basic internal TSF data transfer protection	✓			

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

6.2.1 Class ESM: Enterprise Security Management

ESM_ACD_EXT.1 Access control policy definition
Hierarchical to: No other components.
ESM_ACD_EXT.1.1
The TSF shall provide the ability to define access control policies for consumption by one or more Access Control agents.
ESM_ACD_EXT.1.2
Access control policies defined by the TSF must be capable of containing the following:
a) Subjects: [*end users of the TSF-mediated workstations and servers*]; and
b) Objects: [*files and applications on the TSF-mediated workstations and servers*]; and
c) Operations: [*execute, submit, transmit, view, move, copy, paste, write to*]; and
d) Attributes: [*object criteria as listed in ESM_OAD_EXT.1.1 which match the specified rule properties contained within a defined control or context classification rule*]
ESM_ACD_EXT.1.3
The TSF shall associate unique identifying information with each policy.
Dependencies: No dependencies

ESM_ACT_EXT.1 Access control policy transmission
Hierarchical to: No other components
ESM_ACT_EXT.1.1
The TSF shall transmit policies to compatible and authorized Access Control agents under the following circumstances: [immediately following creation of a new or updated policy, at a periodic interval, [*immediately upon re-establishment of communication with the DG Server*].
Dependencies: ESM_ACD.1 Access control policy definition

ESM_DSC_EXT.1 Object discovery
Hierarchical to: No other components.
ESM_DSC_EXT.1.1
The TSF shall be able to discover objects in the Operational Environment which meet the following conditions: [unencrypted data which policy requires to be encrypted, data which resides in a domain that is inconsistent with the data's defined sensitivity attributes, [*data which meets the sensitivity criteria for classification*]].
ESM_DSC_EXT.1.2
The TSF shall take the following actions upon discovery of an object as defined by ESM_DSC.1.1: [encrypt the object, [*classify the object*]].
Dependencies: No dependencies

ESM_OAD_EXT.1 Object attribute definition
Hierarchical to: No other components.
ESM_OAD_EXT.1.1
The TSF shall maintain the following list of security attributes belonging to individual objects:
[
a) Agent metadata
b) Bus type
c) Drive type
d) Document metadata
e) File classification
f) File name
g) File extension
h) File modified time

i) *File ownership*
j) *File path*
k) *File size*
l) *File metadata*
m) *Network domain*
n) *Network protocol*
o) *Network port*
p) *Network address*
q) *Network transmission direction*
r) *Network URL*
s) *Network metadata*
t) *Process file path*
u) *Process file name*
v) *Process version*
w) *Process MD5 hash*
x) *Process window title*
y) *Process company name*
z) *Process metadata*
aa) *USB device metadata*

].

ESM_OAD_EXT.1.2

The TSF shall be able to associate security attributes with individual objects.

Dependencies: **No dependencies**

6.2.2 Class FAU: Security Audit

FAU_ARP.1 **Security alarms**
Hierarchical to: **No other components**
FAU_ARP.1.1
The TSF shall take
[
The following actions:
a) Log an alert to the Alerts repository
b) Send an email notification to the users subscribed to the alert
]
upon detection of a potential security violation.
Dependencies: **FAU_SAA.1 Potential violation analysis**

FAU_GEN.1(1) **Audit data generation (TOE server)**
Hierarchical to: **No other components.**
FAU_GEN.1(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~~ **core TOE server components, with the aid of the TOE Environment**;
b) All auditable events for the [not specified] level of audit; and
c) [
1. *User management events*
2. *Role management events*
3. *Agent configuration changes*
4. *System configuration changes*
5. *Rule management events*
6. *Policy management events*
7. *Report management and views*
8. *Alert management and views*
9. *Notification subscription events*
10. *Logon failures*
11. *Bundle failures*
12. *Operational alerts*
13. *ETL*[17] *status*

].

Application Note: *The TOE server is comprised of a few Windows services that, with the help of the OS, are capable of generating a startup/shutdown event, which can be viewed in the Windows Event Viewer. Another exception is DGMC Logon failures, which are also captured in the Windows Event Log.*

It should be noted that the DGMC is instantiated as an IIS web application, and therefore does not possess any startup/shutdown auditing capabilities. Regardless, the auditing function is implicit, meaning that it cannot be terminated separately without terminating the TOE server's operation. All of the described auditable events are invoked through the DGMC; even if the web application fails to start or stops suddenly, the auditable events would be prevented from occurring, since they are actions performed by invoking the

[17] ETL – Extract, Transform, Load

application. Thus, there would be no possibility of actions being performed without generating an audit trail.

FAU_GEN.1(1).2

The TSF shall record within each event 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, [*event details*].

Dependencies: **FPT_STM.1 Reliable time stamps**

FAU_GEN.1(2) Audit data generation (TOE agent)

Hierarchical to: **No other components.**

FAU_GEN.1(2).1

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

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

b) All auditable events for the [not specified] level of audit; and

c) [*The auditable events specified in Table 12*].

Table 12 - Auditable Events (TOE agent)

Operation	Auditable Event	Additional Information
Application Data Exchange	*Cut* *Paste* *Insert File* *Insert New Object* *Print Process* *Print Screen* *Screen Capture*	*User* *Computer* *Application*
Application Management	*Application Start*	*User* *Computer* *Application*
File Operations	*Archive* *Copy* *Create* *Decrypt* *Delete* *Edit* *Encrypt* *Move* *Open* *Read* *Recycle* *Rename* *Restore* *Save As* *Write*	*User* *Computer* *Source Path* *Destination Path* *Source File* *Destination File* *Source Drive Type* *Destination Drive Type* *Application*
Logon Activity	*User Logoff* *User Logon*	*User* *Computer* *Authentication mechanism*

Operation	Auditable Event	Additional Information
Mail	*Attach File* *Send Mail*	*Subject* *From* *Recipient* *Recipient Type*
Network Operations	*Network Transfer* *Network Transfer - Download* *Network Transfer - Upload*	*User* *Computer* *IP*[18] *Address* *Protocol* *Direction* *Local Port* *Remote Port* *Application*
Optical Media	*CD Burn*	*User* *Computer* *Application*
Print Spool	*Print*	*User* *Computer* *Application*

FAU_GEN.1(2).2

The TSF shall record within each event record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*the audit relevant information specified in Table 12*].

Dependencies: **FPT_STM.1 Reliable time stamps**

FAU_SAA.1 Potential violation analysis

Hierarchical to: **No other components**

FAU_SAA.1.1

The TSF shall be able to apply a set of rules in monitoring the audited events based on these rules which indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*all events which result in the triggering of a defined control rule*] known to indicate a potential security violation;

b) [*generation of an alert if an event occurs which triggers a control rule designated with an 'alert' response action*].

Dependencies: **FAU_GEN.1(2) Audit data generation (TOE agent)**

FAU_SAR.1(1) Audit review (TOE server data)

Hierarchical to: **No other components**

FAU_SAR.1(1).1

The TSF shall provide [*The System Administrator and other Custom Roles defined by the System Administrator*] with the capability to read [*the auditable events defined in FAU_GEN.1(1).1*] from the audit records.

FAU_SAR.1(1).2

[18] IP – Internet Protocol

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: **FAU_GEN.1(1) Audit data generation (TOE server)**

FAU_SAR.1(2) **Audit review (TOE agent data)**

Hierarchical to: **No other components**

FAU_SAR.1(2).1

The TSF shall provide [*the authorized roles in Table 13*] with the capability to read [*the information specified in Table 13*] from the event records.

Table 13 - Audit Review (TOE agent data)

Data	Authorized roles
Real-time event data (Local Reports)	*Local Report Viewer* *System Administrator* *Other Custom Roles specified by the System Administrator*
Historical event data (Enterprise Reports, Trend Reports, Dashboard Reports, Data-At-Rest Reports, Operational Alerts, ETL Status)	*Enterprise Report Viewer* *System Administrator* *Other Custom Roles specified by the System Administrator*
Alert data	*Alert Manager* *System Administrator* *Other Custom Roles specified by the System Administrator*

FAU_SAR.1(2).2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: **FAU_GEN.1(2) Audit data generation (TOE agent)**

6.2.3 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.
FCS_CKM.1.1
The TSF shall generate **symmetric** cryptographic keys in accordance with a specified **deterministic random bit** ~~cryptographic key~~ generation algorithm [*Hash-DRBG*] and specified cryptographic key sizes [*128, 192, 256*] that meets the following: [*NIST Special Publication 800-90*].
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4 Cryptographic key destruction
Hierarchical to: No other components.
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*].
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.
FCS_COP.1.1
The TSF shall perform [*the operations listed in Table 14*] in accordance with a specified cryptographic algorithm [*the ciphers listed in Table 14*] and cryptographic key sizes [*the key sizes listed in Table 14*] that meets the following: [*standards listed in Table 14*].
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

Application Note: *The VSEC module has been awarded CMVP validation certificate #1607. Refer to the following for more information:*

- *Consolidated Certificate:*
  - *http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/FIPS140ConsolidatedCertList0009.pdf*
- *Security Policy:*
  - *http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1607.pdf*

Table 14 - Cryptographic Services

Operation	Algorithm	Key Sizes	Standards
Encryption/Decryption	AES-CBC[19]	128 192 256	FIPS PUB[20] 197 NIST Special Publication 800-57 NIST Special Publication 800-38A
	AES-CTR AES-ECB[21]	256	
Key Wrapping	RSA	2048 3072 4096	NIST Special Publication 800-56B
Signature Generation	rDSA	2048 3072 4096	FIPS PUB 186-3
Signature Verification	rDSA	1024 1536 2048 3072 4096	FIPS PUB 186-3
Cryptographic Hashing	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	160 224 256 384 512	FIPS PUB 180-3
Keyed-Hash Message Authentication	HMAC[22]-SHA-1 HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	160 224 256 384 512	FIPS PUB 198-1 FIPS PUB 180-3

[19] CBC – Cipher Block Chaining
[20] PUB - Publication
[21] ECB – Electronic Codebook
[22] HMAC – Hash-based Message Authentication Code

6.2.4 Class FDP: User Data Protection

FDP_ACC.1(1) **Subset access control (TOE server)**
Hierarchical to: **No other components.**
FDP_ACC.1(1).1

The TSF shall enforce the [*Management Access Control SFP*] on [*the subjects, objects, and operations listed in Table 15*]

Table 15 - Management Access Control SFP

Subject	Object	Operation
DGMC User	*DGMC Users* *DGMC Roles* *DGMC Rules* *DGMC Policies* *DGMC Reports* *DGMC Notifications* *DGMC Configuration Data*	*View* *Create* *Modify* *Delete*
	DGMC Events	*View*
	DGMC User Interface Elements	*View/Interact*

Dependencies: **FDP_ACF.1(1) Security attribute based access control (TOE server)**

FDP_ACC.1(2) **Subset access control (TOE agent)**
Hierarchical to: **No other components.**
FDP_ACC.1(2).1

The TSF shall enforce the [*Enterprise Information Protection SFP*] on [*the subjects, objects, and operations listed in Table 16*]

Table 16 - Enterprise Information Protection SFP

Subject	Object	Operation
DG Agent User	*Application*	*Execute*
	Application Data	*Cut* *Paste* *Insert File* *Insert New Object* *Print Process* *Print Screen* *Screen Capture*
	Email	*Attach File* *Send Mail*
	File	*Archive* *Copy* *Create* *Decrypt* *Delete*

Subject	Object	Operation
		Edit *Encrypt* *Move* *Open* *Read* *Recycle* *Rename* *Restore* *Save As* *Write*
	Optical Media	*CD Burn*
	Print Spool	*Print*
	Network Data	*Transfer* *Upload* *Download*

Application Note: *The intent of the Enterprise Information Protection SFP is to ensure that data defined as proprietary or sensitive according to its context should not be able to leave a computer through some set of common means. For example, the TSF should prevent data from being exported to a different logical drive unless explicitly allowed.*

Application Note: *The TOE provides a capability of examining the Operational Environment for unencrypted or misplaced sensitive data and correcting the discrepancy. This capability is represented by the ESM_DSC_EXT.1 SFR.*

Dependencies: **FDP_ACF.1(2) Security attribute based access control (TOE agent)**

FDP_ACF.1(1) **Security attribute based access control (TOE server)**

Hierarchical to: **No other components.**

FDP_ACF.1(1).1

The TSF shall enforce the [*Management Access Control SFP*] to objects based on the following: [*DGMC user ID, DGMC user password, DGMC role membership, DGMC role privilege levels*].

FDP_ACF.1(1).2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

1. *If the subject has the System Administrator role, access is granted*
2. *If a subject who does not have the System Administrator role requests access to an object that requires permissions, the permissions of the subject's assigned role are examined to determine if the subject has permission to access the object. If a match is found, access is granted*
3. *If none of the above rules apply, access is denied*

].

FDP_ACF.1(1).3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1(1).4

The TSF shall explicitly deny access of subjects to objects based on the [*no additional rules*].

Dependencies: **FDP_ACC.1(1) Subset access control (TOE server)**
FMT_MSA.3 Static attribute initialization

FDP_ACF.1(2) Security attribute based access control (TOE agent)
Hierarchical to: **No other components.**

FDP_ACF.1(2).1

The TSF shall enforce the [*Enterprise Information Protection SFP*] to objects based on the following: [*the object attributes defined in ESM_OAD_EXT.1*].

FDP_ACF.1(2).2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

Control rules contained within a policy applied to a subject, encompassing the following notions:

a) Attributes of environmental data may be marked with an attribute such as sensitive or proprietary based on contextual criteria, not otherwise allowed to be disclosed; and

b) Objects which are classified as sensitive based on contextual criteria will be forbidden from leaving the system unless the intended destination is an explicitly trusted location; and

c) Mechanisms of leaving the system will constitute, at minimum, transfer to other logical devices, network locations, printing, emailing, and copying to clipboard.

d) Upon triggering a control rule, the following configurable actions may be carried out:

i. Block the operation

ii. Continue the operation and generate an alert

iii. Encrypt the file associated with the user action

iv. Prompt the user and perform the following actions:

a. *Block – Terminates the user's action*
b. *Decide – Allows the user to decide whether or not to continue*
c. *Warn – Allows the user to continue, but issues a warning to the user*
d. *Justify – Allows the user to continue, but the user is required to enter a response as justification for the action*

v. Vault the operation and apply an additional set of rules

].

Application Note: *Contextual criteria include application executable names and versions, file extensions, source and destination locations, files intended for email attachment, files intended for printing, source and destination applications, etc.*

Application Note: *Sensitivity attributes may include the types of objects which are controlled by the SFP, such as "Human Resources", "Financial", or "Source Code" data. These are based on file extensions, e.g. .c and .h files (for source code files), or a combination of file extension and source location, e.g. .xls files residing on a network share designated as a repository for financial statements.*

FDP_ACF.1(2).3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*if the operation being performed is explicitly flagged as trusted by a filter rule, the operation will be allowed*].

FDP_ACF.1(2).4

The TSF shall explicitly deny access of subjects to objects based on the [*no additional rules*].

Dependencies: **FDP_ACC.1(2) Subset access control (TOE agent)**
FMT_MSA.3 Static attribute initialization

FDP_ITC.1 Import of user data without security attributes

Hierarchical to: **No other components.**

FDP_ITC.1.1

The TSF shall enforce the [*Management Access Control SFP*] when importing ~~user data,~~**asymmetric keys for use in the VSEC module** controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*the ability to import private keys shall be restricted to users with the System Administrator role, or to personnel performing the installation and initial configuration of the TOE*].

Dependencies: **[FDP_ACC.1(1) Subset access control (TOE server), or**
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

6.2.5 Class FIA: Identification and Authentication

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

Application Note: *The intent of this SFR is to require authentication for users of the DGMC. The TSF does not perform authentication of users on workstations and servers the TOE is intended to protect; rather, it is expected that users in the TOE Environment will be authenticated by a mechanism provided by the OS of the TSF-mediated system, using local or centrally stored user accounts, such as those provided by an LDAP repository.*

Dependencies: **FIA_UID.1 Timing of identification**

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

Application Note: *The intent of this SFR is to require identification for users of the DGMC. While the TOE does retrieve identity information for users of the TSF-mediated systems, it is not under the scope of the TOE's capabilities to maintain a repository containing user identity attributes for subjects in the TOE Environment; rather, identity information is provided by the OS of the TSF-mediated system, using local or centrally stored accounts, such as those provided by an LDAP repository. The TOE uses the identity information provided to it to associate events with the user performing the action that caused the event.*

Dependencies: **No dependencies**

6.2.6 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour
Hierarchical to: No other components.
FMT_MOF.1.1

The TSF shall restrict the ability to [**Take the actions listed in Table 17**] the functions [*security functions listed in Table 17*] to [*the roles listed in Table 17*].

Table 17 - Management of Security Functions Behavior

Security Function	Actions	Authorized Roles
Management of Users and Roles	*Determine the behavior of* *Modify the behavior of* *Enable* *Disable*	*System Administrator* *Other Custom Roles specified by the System Administrator*
Management of Alerts	*Determine the behavior of* *Modify the behavior of* *Enable* *Disable*	*System Administrator* *Alert Manager* *Other Custom Roles specified by the System Administrator*
Management of Classification Rules and Policies	*Determine the behavior of* *Modify the behavior of* *Enable* *Disable*	*System Administrator* *Classification Policy Manager* *Other Custom Roles specified by the System Administrator*
Management of Control Rules and Policies	*Determine the behavior of* *Modify the behavior of* *Enable* *Disable*	*System Administrator* *Control Policy Manager* *Other Custom Roles specified by the System Administrator*
Management of Filter Rules and Policies	*Determine the behavior of* *Modify the behavior of* *Enable* *Disable*	*System Administrator* *Filter Policy Manager* *Other Custom Roles specified by the System Administrator*
Management of Trusted Process Rules and Policies	*Determine the behavior of* *Modify the behavior of* *Enable* *Disable*	*System Administrator* *Trusted Process Policy Manager* *Other Custom Roles specified by the System Administrator*
Management of Local Reports	*Determine the behavior of* *Modify the behavior of*	*System Administrator* *Local Report Viewer* *Other Custom Roles specified by the System Administrator*
Management of Enterprise Reports	*Determine the behavior of* *Modify the behavior of*	*System Administrator* *Enterprise Report Viewer* *Other Custom Roles specified by the System Administrator*
Management of Events	*Determine the behavior of* *Modify the behavior of* *Enable* *Disable*	*System Administrator* *Other Custom Roles specified by the System Administrator*
Management of System Configuration	*Determine the behavior of* *Modify the behavior of* *Enable* *Disable*	*System Administrator* *Other Custom Roles specified by the System Administrator*
Management of DG Agent Operation	*Determine the behavior of*	*System Administrator*

Security Function	Actions	Authorized Roles
	Modify the behavior of *Enable* *Disable*	*Other Custom Roles specified by the System Administrator*
Management of Email Notification Configuration	*Determine the behavior of* *Modify the behavior of* *Enable* *Disable*	*System Administrator* *Other Custom Roles specified by the System Administrator*

Application Note: *The intent of this SFR is to ensure that users under the scope of TSF control cannot interfere with the operation of the TOE by attempting to modify the behavior of it through its management interfaces.*

Application Note: *The TOE is capable of cloaking the DG Agent processes and configuration to avoid inspection from an unprivileged user, as well as providing tamper protection to resist being terminated or modified by the users under the scope of TSF control.*

Application Note: *Management users (DGMC Users) and users in the Operational Environment are considered to be in separate domains; therefore it is necessary to possess administrative rights on the workstations and servers on which the DG Agents are installed, along with the proper tools for performing maintenance or troubleshooting of the DG Agent software. In order to terminate or uninstall DG Agent processes, a shared secret must be used.*

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

FMT_MSA.1 **Management of security attributes**
Hierarchical to: **No other components.**
FMT_MSA.1.1

The TSF shall enforce the [*Management Access Control SFP*] to restrict the ability to [**the operations defined in Table 18**] the security attributes [*the security attributes defined in Table 18*] to [*the authorized roles defined in Table 18*].

Table 18 - Security Attributes

Operation	Security Attribute	Authorized roles
Change default Query Modify *No other operations*	*DGMC User ID*	*System Administrator* *Other Custom Roles specified by the System Administrator*
Change default Modify *No other operations*	*DGMC User Password*	*System Administrator* *Other Custom Roles specified by the System Administrator*
Change default Query Modify Delete *No other operations*	*DGMC Role Membership*	*System Administrator* *Other Custom Roles specified by the System Administrator*
Change default	*DGMC Role Privilege*	*System Administrator*

Operation	Security Attribute	Authorized roles
Query Modify Delete *No other operations*	*Levels*	*Other Custom Roles specified by the System Administrator*
Change default Query Modify Delete *No other operations*	*Policy Rules*	*System Administrator* *Classification Policy Manager (Classification Policies)* *Control Policy Manager (Control Policies)* *Filter Policy Manager (Filter Policies)* *Trusted Process Policy Manager (Trusted Process Policies)* *Other Custom Roles specified by the System Administrator*
Change default Query Modify Delete *No other operations*	*Rule Properties*	*System Administrator* *Classification Policy Manager (Classification Rules)* *Control Policy Manager (Control Rules)* *Filter Policy Manager (Filter Rules)* *Trusted Process Policy Manager (Trusted Process Rules)* *Other Custom Roles specified by the System Administrator*
Change default Query Modify Delete *No other operations*	*Notification Subscriptions*	*Alerts Manager* *System Administrator* *Other Custom Roles specified by the System Administrator* *User of Origin (Private Notifications)*

Dependencies: **[FDP_ACC.1(1) Subset access control (TOE server) or FDP_IFC.1 Subset information flow control]**
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 **Static attribute initialisation**
Hierarchical to: **No other components.**
FMT_MSA.3.1

The TSF shall enforce the [*Management Access Control SFP*] to provide [**the properties defined in Table 19**] default values for security attributes that are used to enforce the SFP.

Table 19 - Security Attribute Value Properties

Security Attribute	Property
DGMC User ID	N/A
DGMC User Password	N/A
DGMC Role Membership	Restrictive
DGMC Role Privilege Levels	Restrictive

Security Attribute	Property
Policy Rules	Permissive
Rule Properties	Permissive
Notification Subscriptions	Permissive

FMT_MSA.3.2

The TSF shall allow the [*roles specified in Table 18*] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: **FMT_MSA.1 Management of security attributes**
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: **No other components.**

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:

[

a) management of users and roles
b) alert management
c) management of classification rules and policies
d) management of control rules and policies
e) management of filter rules and policies
f) management of trusted process rules and policies
g) management of enterprise reports
h) management of local reports
i) event management
j) management of notification configuration
k) management of system configuration
l) management of agent configuration

].

Dependencies: **No dependencies**

FMT_SMR.1 Security roles

Hierarchical to: **No other components.**

FMT_SMR.1.1

The TSF shall maintain the roles

[

a) System Administrator
b) Alert Manager
c) Classification Policy Manager
d) Control Policy Manager
e) Enterprise Report Viewer
f) Filter Policy Manager
g) Local Report Viewer
h) Trusted Process Policy Manager
i) Other Custom Roles containing privilege levels defined by the System Administrator

].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: **FIA_UID.1 Timing of identification**

6.2.7 Class FPT: Protection of the TSF

FPT_FLS.1 **Failure with preservation of secure state**
Hierarchical to: **No other components.**
FPT_FLS.1.1
The TSF shall preserve a secure state when the following types of failures occur: [*disruption of DG Agent network connectivity; DG Database failure*].

Application Note: *In the first failure scenario, the DG Agent is capable of continuing the enforcement of the TOE access control policies when the communications link between DG Agent and DG Server is broken. Immediately upon reestablishment of connectivity, the DG Agent will retrieve the most recently assigned policies. The DG Agent will preserve the bundle data until it has successfully re-established a connection with the DG Server. In the second scenario, if the DG Server encounters an error writing to the DG Database, the DG Server generates an error in the Windows event log, informing the TOE administrator that a fault has occurred.*

Dependencies: **No dependencies.**

FPT_ITT.1 **Basic internal TSF data transfer protection**
Hierarchical to: **No other components.**
FPT_ITT.1.1
The TSF shall protect TSF data from [*disclosure*] when it is transmitted between separate parts of the TOE.

Application Note: The TOE agent leverages its FIPS 140-2 validated VSEC module to generate symmetric AES-256 keys and encrypt TSF data (forensic data bundles) as necessary to support the FPT_ITT.1 claim. The VSEC module protects the symmetric keys using RSA-2048 asymmetric encryption keys, which are generated by the cryptographic providers in the TOE environment.

Dependencies: **No dependencies**

6.2.8 Class FRU: Resource Utilization

FRU_FLT.1 **Degraded fault tolerance**
Hierarchical to: **No other components.**
FRU_FLT.1.1

The TSF shall ensure the operation of [*access control policy enforcement, preservation of agent forensic activity bundles*] when the following failures occur: [*disruption of DG Agent network connectivity*].

Application Note: *The DG Agent is capable of continuing the enforcement of the TOE access control policies when the communications link between DG Agent and DG Server is broken. Immediately upon reestablishment of connectivity, the DG Agent will retrieve the most recently assigned policies. In addition, the DG Agent will preserve the bundle data until it has successfully re-established a connection with the DG Server.*

Dependencies: **FPT_FLS.1 Failure with preservation of secure state**

6.2.9 Class FTA: TOE Access

FTA_SSL.3 **TSF-initiated termination**
Hierarchical to: **No other components.**
FTA_SSL.3.1
The TSF shall terminate an interactive session after a [*System Administrator-configurable time interval*].

Application Note: *This time interval refers to the DGMC Idle Timeout value and does not apply to user sessions on TSF-mediated machines in the TOE Environment.*

Dependencies: **No dependencies**

FTA_TAB.1 **Default TOE access banners**
Hierarchical to: **No other components.**
FTA_TAB.1.1
Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.
Dependencies: **No dependencies**

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 20 - Assurance Requirements summarizes the requirements.

Table 20 - Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7 TOE Summary Specification

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

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements. Table 21 lists the security functions and their associated SFRs.

Table 21 - Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Robust Security Management	FAU_GEN.1(1)	Audit data generation (TOE server)
	FAU_SAR.1(1)	Audit review (TOE server data)
	FDP_ACC.1(1)	Subset access control (TOE server)
	FDP_ACF.1(1)	Security attribute based access control (TOE server)
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
	FTA_SSL.3	TSF-initiated termination
	FTA_TAB.1	Default TOE access banners
Enterprise Information Protection	ESM_ACD_EXT.1	Access control policy definition
	ESM_ACT_EXT.1	Access control policy transmission
	ESM_DSC_EXT.1	Object discovery
	ESM_OAD_EXT.1	Object attribute definition
	FDP_ACC.1(2)	Subset access control (TOE agent)
	FDP_ACF.1(2)	Security attribute based access control (TOE agent)
	FPT_ITT.1	Basic internal TSF data transfer

TOE Security Function	SFR ID	Description
		protection
Cryptographic Protection	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
	FDP_ITC.1	Import of user data without security attributes
Violation Analysis, Alerting, and Reporting	FAU_ARP.1	Security alarms
	FAU_GEN.1(2)	Audit data generation (TOE agent)
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1(2)	Audit review (TOE agent data)
Fault Tolerance	FPT_FLS.1	Failure with preservation of secure state
	FRU_FLT.1	Degraded fault tolerance

7.1.1 Robust Security Management

The DG Server implements the Management Access Control SFP, based on a defined set of security attributes which determine the behavior of the TSF. The modification of attribute values is restricted to appropriately authorized roles. In addition, it restricts attribute values to restrictive or permissive defaults, where appropriate. Security attributes used to enforce the Management Access Control SFP include: user IDs, passwords, role memberships, role privilege levels, policy rules, rule properties, and alert notification subscriptions.

The DG Server enforces identification and authentication for users of the DGMC. Subjects are required to enter a valid username, password, and domain prior to being presented with DGMC user interface elements. No anonymous access is provided. Interface elements displayed to the user are based on the user's authorized roles/privilege levels, which are discussed later in this section.

Users as they pertain to TOE functions are divided into three classes: DGMC Users, DG Agent Users, and Administrators (users with full administrative privileges to the TOE). DGMC Users may contain a subset of privileges used to manage the TOE through the DGMC. DG Agent Users are end-users of the TSF-mediated workstations and servers and do not interact directly with the TOE (unless prompted by the DG Agent). DG Agent Users are only identified by the TOE, not authenticated. DGMC Users and Administrators define the operations permitted for DG Agent Users. Administrators may be considered a subset of DGMC Users, but also contain privileges outside the DGMC realm, such as TOE installation, configuration, and maintenance. Within the DGMC realm, Administrators would be considered users with the "System Administrator" role. Outside, they could refer to TOE application server administrators, TOE database administrators, or individuals who possess the service account credentials for running TSF-dependent services.

The DG Server provides methods for authenticated, authorized DGMC Users and Administrators to:

- Create and manage DGMC Users and roles
- Install and maintain DG Agents
- Create DG Rules that record and respond to specific DG Agent User actions
- Create and apply DG Policies to DG Agent Users

- View and resolve DG Alerts triggered by DG Rules in DG Policies
- View DG Reports that contain user activity data

DGMC Users and Administrators access the DGMC using a web browser installed on the management workstation using a secure HTTPS connection. The DG Server enforces strict session security for users of the DGMC. Each time a DGMC User accesses the DG Server, an advisory warning is displayed to the user prior to identification and authentication. DGMC User sessions are automatically terminated after an Administrator-configurable time period.

The DG Server enforces role-based access control for DGMC Users using a pre-defined set of System Roles. The following System Roles are provided:

- **Alert Manager** – Access to the *Alerts* tab; can view and resolve DG Alerts.
- **Classification Policy Manager** – Access to the *Classification* tab; Creates Classification rules, policies, and content patterns. Imports new dictionary files and query files.
- **Control Policy Manager** – Creates and administers rules that apply to Control Policies, which are used to govern user actions.
- **Enterprise Report Viewer** – Access to enterprise level reports; Views reports drawing on historical data in the Reporting database.
- **Filter Policy Manager** – Creates and administers rules that apply to Filter Policies. Applies Filter Policies to users, groups, and computers.
- **Local Report Viewer** – Access to the local DGMC forensic report, drawing on real-time data in the Collection database.
- **System Administrator –** Access to all areas of DGMC; assigns roles to other DGMC Users and receives Operational Emails in response to specific events.
- **Trusted Process Policy Manager –** Creates and administers rules that apply to Trusted Process Policies.

System Roles are pre-defined collections of security attributes, or privilege levels, which can be assigned to any user. Privilege levels extend the basic authorization provided by the System Roles by allowing the creation of Custom Roles, which could contain any combination of privilege levels. In Digital Guardian vernacular, privilege levels translate to operations, which are mapped to objects. These privilege levels are then assigned to a role, which in turn is assigned to DGMC Users through role membership. DGMC Users may be assigned to one or more roles simultaneously. The resulting privileges amount to a union of all privilege levels contained within the user's assigned roles.

The TOE enforces access to DGMC elements based on the following privilege levels:

- **None –** User has no access to the item (object); the object will not appear in the user's DGMC session.
- **Read All –** User has read only access to the object; user can view the object, but cannot interact with it.
- **Modify All –** User can view and edit existing objects of this type.
- **Create All –** User can view, edit, and create objects of this type.
- **Full Control –** User has complete privileges for this object, including delete privileges, if they exist for the specified object.

The complete list of objects/actions that can be mapped to privilege levels is outlined in the *Using Digital Guardian* guidance document in the section entitled "About Privilege Levels".

Aside from providing access control to DGMC management functions, the DG Agent is able to enforce the Management Access Control SFP on end-users of the TOE by preventing them from observing or disabling the agent software. Because the DG Agent contains a kernel-level process that injects itself into running processes, it is able to maintain low-level system control of the TOE operating environment. The DG Agent treats running processes differently based on process flags, which it applies to Digital Guardian processes. Process flags for tamper protection include invisibility, which makes the process transparent to

the user; immortality, which prevents users from terminating the process; and a "stealth" mode, which hides all traces of agent activity, along with configuration files and DG Agent executables, however, impacts system performance.

All management activity performed through the DGMC, including user/role management, policy/rule management, report management, alert/event management, and system configuration events, are recorded by the DG Server and stored within the DG database. Audit records are viewable by the System Adminstrator using the Console Activity report. The audit records contain the information fields explained in Table 22:

Table 22 - Audit Record Contents

Field	Content
Date	Date and time of the event
User	Identity of the subject performing the operation
Category	Type of operation being performed
Detail	Additional information about the event

TOE Security Functional Requirements Satisfied:
FAU_GEN.1(1), FAU_SAR.1(1), FDP_ACC.1(1), FDP_ACF.1(1), FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1, FTA_SSL.3, FTA_TAB.1

7.1.2 Enterprise Information Protection

The DG Agents enforce access control for users of the TSF-mediated workstations and servers using a set of rules as defined within a policy associated with the machine or user on which the DG Agent is installed. DG Agents are capable of mediating several types of user and application activity, including:

- Application Data Exchange (ADE) events – copying/pasting of sensitive data from one application to another
- Application start events – launching a specific executable
- CD/DVD burn events – copying data files and writing them to a recordable optical drive
- Email events – sending email attachments to a recipient outside the organization, to an unapproved domain, or to an unauthorized recipient within an organization
- File events – deleting/copying files
- Network events – file uploads and downloads
- Print events – sending sensitive documents to the print spooler

DG Rules govern the decisions made by the DG Agent for the various event types. Rule definitions at the base level consist of an event operation and a property. Event operations use symbolic constants to define the rule-governing event. The rule property defines the condition which must be met in order to trigger the rule. Rules can take the form of one of several enforcement types:

- Application Management Rules
- Control Rules
- Classification Rules
- Filter Rules
- Trusted Process Rules
- Data Vault Rules
- Component Rules

Application Management Rules govern the use of authorized and unauthorized applications that run in the TOE environment. An application management rule can be used to block instant messaging or peer to peer applications, for example. For this type of rule, the actions which can be taken include: *Undecided, Allow,* or *Control*. *Undecided* flags the processes for further investigation whilst allowing the execution, *Allow* permits the application to run without flagging it, and *Control* blocks the execution either transparently or accompanied with a notification to the end user informing them that the application was blocked. When an application event occurs, the TOE records the name of the executable file, the file version, the file's publisher, and an MD5 hash of the file. This information can then be used to build application white lists and black lists based on unique application properties.

Control Rules govern authorized and unauthorized user actions. An example would be blocking a user from writing sensitive data files to a CD. Actions to be taken include *Block, Continue, Encrypt, Vault,* and *Prompt.*

- *Block* expressly denies the action without prompting, with an optional notification message informing the user that the action was blocked.
- *Continue* allows the activity, but generates an alert which can optionally be sent to an Administrator or DGMC User.
- *Encrypt* leverages the AFE module to encrypt the associated file. If the AFE feature is not enabled on the machine on which the DG Agent runs, the action results in a *Block* if the rule is set to *Encrypt.*
- *Vault* allows the action to continue, but an additional set of rules is enforced upon triggering of the rule.
- The *Prompt* action displays a message to the user indicating that the action is being recorded, and blocks or allows the action depending on the prompt settings, which include: *Block, Decide, Justify, and Warn.*
    - *Block* expressly denies the action, while *Decide, Justify,* and *Warn* allow the action at the user's discretion.
    - *Decide* gives the user an opportunity to stop the operation from continuing.
    - *Justify* requires the user to enter a justification for the requested action.
    - *Warn* permits the action but informs the user that the activity is logged.

Classification Rules contain a set of criteria for classifying files. For example, a classification rule could identify files with a *.pst* extension as an archive file containing mail items, or *.c* and *.h* extensions as proprietary source code files. Classification Rules are used in conjunction with Control Rules that specify a behavior for classified files. This type of rule is not triggered by an event, rather, it is used when the DG Scanner performs discovery of files in the TOE environment, and classifies them based on the context classification properties.

Filter Rules prevent the DG Agent from processing events specified in the rule. Filtered events are still tracked and regulated by Control Rules; however, they are excluded from reports. A filter rule could be used to inhibit processing of actions performed on a set of unclassified public documents. DG Agents employ Implicit Filtering to automatically remove low-level system activity based on file extensions and signatures, as well as Administrator-defined rules that are based on the same properties used in Control Rules and Trusted Process Rules.

Trusted Process Rules prevent the DG Agent from recording activity related to a specific process. For example, an anti-virus application or host-based firewall might be considered a trusted process.

Data Vault Rules add an extra layer of security to existing rules. This type of rule takes effect when conditions outlined in a trigger rule have been met. For example, a rule could trigger a data vault when a sensitive application is executed, and any uploads, writes to CD, or file save activities outside of a specified directory might be prevented until the application is unloaded from memory.

Component Rules are rule definitions that can be referenced from within another rule of the same type. This type of rule would be useful for re-using rule definitions, such as classification rules for sensitive file types.

Once a set of rules have been defined, they can be logically organized according to rule categories. To enforce the rules, they must be associated with a policy. Policies are containers for a set of rules that are applied to user and computer objects or groups of objects. User policies are applied at logon, while computer policies are applied at startup, allowing for a baseline enforcement of system-level policy. User and computer object information can be generated using Windows Networking or through synchronization with an external LDAP server.

DG Agents are capable of enforcing the following policy types:

- Control Policies – Contain a set of Control Rules governing user actions, such as file activities or clipboard operations
- Classification Policies – Contain a set of Classification Rules which identify and flag files meeting set criteria.
- Filter Policies – Contain a set of Filter Rules that exclude specific activity that TOE Administrators do not wish to track.
- Trusted Process Policies – Contain a set of Trusted Process Rules used to filter out events generated by known safe processes.

By default, a Default User Policy is enforced, which applies a Control Policy to users with no other assigned policies. This ensures enterprise-wide protection for users who have not yet been assigned to a DG Policy. Typically, a Default Policy contains the most restrictive rules. All DG Agent computers are automatically assigned to this policy.

To deal with potential policy confliction, for example, a policy that contains a *Block* rule and an *Allow* rule for the same operation, rules are assigned a priority value. The DG Agent starts with the lowest priority value first, and proceeds in an ascending order. A common scenario is when a policy containing a set of rules is enforced at a system-wide level on a computer to block all write access to optical drives. If a user policy authorizes a user for write access, and the user logs on to the workstation, their privilege would be denied, unless the policy granting the user access is prioritized and enforced first in order, allowing the user privilege to be applied rather than the system-level policy.

DG Agents communicate regularly with the DG Server to upload forensic activity bundles and retrieve up-to-date policies, ensuring that the most current policies are enforced on systems in the TOE environment, and that the forensic event data collected by them is readily available to TOE administrators. To protect the transmitted bundle data from disclosure, the VSEC module generates two symmetric AES-256 session keys; one which is used to encrypt bundle data uploaded to the DG Server, and the other which is used to encrypt return data, including policies, configuration files, and agent instructions. The DG Agent encrypts the symmetric key used for bundle encryption with the DG Server's public RSA-2048 key and transmits the wrapped key, along with the encrypted bundle, to the DG Server. In addition, the DG Agent signs the bundle data using its private RSA-2048 key. The RSA-2048 keys used by the DG Agent are generated by the BCRYPTPRIMITIVES provider on the DG Server, and distributed, along with the DG Server's public key, to the DG Agent during registration.

Typically, the DG Agent examines files in motion or in use, however, it does not interact with files that the user is not interacting with. For features like AFE, the DG Scanner is used to actively scan the contents of the local hard drive to classify or encrypt files based on Classification or Control Rules. Control Rules are enforced by a set of contextual object properties

TOE Security Functional Requirements Satisfied:
ESM_ACD_EXT.1, ESM_ACT_EXT.1, ESM_DSC_EXT.1, ESM_OAD_EXT.1, FDP_ACC.1(2), FDP_ACF.1(2), FPT_ITT.1

7.1.3 Cryptographic Protection

The FIPS 140-2 validated VSEC module provides symmetric key generation, symmetric encryption/decryption, key transport, digital signatures, cryptographic hashing, and keyed-hash message authentication functions using approved ciphers and key sizes, in accordance with approved government standards. Symmetric keys are generated using an approved deterministic random bit generator (DRBG) and are zeroized from memory buffers according to FIPS requirements. Asymmetric keys are imported from an existing PKI during installation of the TOE. The VSEC module is utilized to provide cryptographic operations requested by the AFE and RME modules, and to protect bundle data transmitted to the DG Server from disclosure.

The full list of ciphers/key lengths in use by the VSEC module are listed in Table 23 below:

Table 23 - FIPS-Approved Algorithms

Algorithms/Key Sizes
AES–CBC with 128, 192, and 256 bit key sizes, AES- CTR, ECB with 256 bit key sizes
RSA (RSASSA[23]-PKCS1[24]-v1_5) Key Wrapping – 2048, 3072, 4096 bit key sizes
RSA (RSASSA-PKCS1-v1_5) Signature Generation – 2048, 3072, 4096 bit key sizes
RSA (RSASSA-PKCS1-v1_5) Signature Verification – 1024, 1536, 2048, 3072, 4096 bit key sizes
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512
NIST Special Publication 800-90 Hash_DRBG

For more information on the VSEC cryptographic implementation, please refer to the *Verdasys Secure Cryptographic Module v1.0 FIPS 140-2 Non-Proprietary Security Policy*.

TOE Security Functional Requirements Satisfied:
FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FDP_ITC.1

7.1.4 Violation Analysis, Alerting, and Reporting

The DG Agent generates events for all types of actions the TOE is capable of monitoring, such as file operations or application operations. These events are assembled into collections, known as bundles, and sent to the DG Server to be recorded into the Collection database. All events contain a timestamp, which is provided by the kernel of the underlying Windows OS.

Control Rules and Application Management Rules which govern the behavior of end-users and applications in the TOE environment have the option of generating an alert when a particular event threshold is met or if a rule is violated, such as any operation which results in a *Block* action. When these types of rules are

[23] RSASSA – RSA Signature Scheme with Appendix
[24] PKCS1 – Public-Key Cryptography Standard #1

triggered, an alert is created and added to the Alerts database. Notifications are sent by the DG Server via SMTP to a DGMC User who has subscribed to that alert.

Notifications are divided into three categories: Public, Private, and System. DGMC Users create Public Notifications to which any user can subscribe. Private Notifications are only able to be subscribed to by the DGMC User who created the notification. System Notifications are sent to TOE Administrators when a system error condition or failure occurs resulting in an alert. DGMC Users with the Alert Manager privileges can assign Public and System Notifications to DGMC Users by their DG Roles, or to external recipients outside of the DG domain via email address.

Each notification provides the recipient with information on the alert, error condition, or failure, which contains the necessary details to aid in an investigation of the root issue. Alerts are selectable on a per-user basis, allowing DGMC Users to reduce the number of emails generated when an alert occurs. Each Control Rule has an associated severity level, which determines the risk associated with a violation of the rule. DGMC Users can choose to subscribe to alert notifications based on the assigned severity levels. For example, a DGMC User may subscribe to alerts with a severity level of *Critical*, resulting in notification of only the violations that pose the highest risk to an organization.

Using the Reporting feature, authorized DGMC Users view events based on several factors, including users, time period, or severity level. Alerts are then analyzed by an Alert Manager and resolved to remove them from the list of alerts. Alert investigators assign resolution codes to indicate that the alert was analyzed and processed. Possible alert codes could be assigned to indicate the level of risk, such as No Risk, Possible Risk, or Data Leak, or to indicate how the alert was responded to, such as No Response, Policy Change, Employee Warned, or Employee Terminated.

Table 24 lists the information fields and the contents of each field contained within an event record:

Table 24 - Event Record Contents

Field	Content
Date	Date and time of the event
Operation	Activity which was performed
User	Identity of the subject performing the operation
Computer	Machine running the agent which observed the event
Application	Executable name of the application involved in the event
Category	Type of operation being performed
Detail	Additional information about the event

TOE Security Functional Requirements Satisfied:
FAU_ARP.1, FAU_GEN.1(2), FAU_SAA.1, FAU_SAR.1(2)

7.1.5 Fault Tolerance

In the event of a communications outage between the DG Server and DG Agent, such as when a laptop user is offline, the DG Agent will continue enforcement of the most recently applied policy. Upon re-connection to the enterprise network, the DG Agent will immediately check for and download any changes to the policy which may have occurred during the outage. Any bundle data generated is preserved by the DG Agent until it can successfully re-establish communication with the DG Server.

In the event that the DG Server is unable to write DG Agent bundle data to the DG Database, the DG Server writes an error to the Windows event log.

TOE Security Functional Requirements Satisfied:
FPT_FLS.1, FRU_FLT.1

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3.

8.2 Security Objectives Rationale

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

8.2.1 Security Objectives Rationale Relating to Threats

Table 25 below provides a mapping of the objects to the threats they counter.

Table 25 - Threats:Objectives Mapping

Threats	Objectives	Rationale
T.ADMIN_ERROR An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security enforcement mechanisms.	NOE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	NOE.MANAGE ensures that the individuals intended to deliver, install, manage, and operate the TOE are carefully selected, properly trained, and follow all IT Security practices.
T.DISABLE A malicious or careless user may suspend or terminate the TOE agent's operation, rendering its ability to mediate access control upon the TOE environment or protected data useless.	O.RESILIENT The TOE agent must prevent users in the Operational Environment from performing actions that would disable or otherwise modify its behavior.	O.RESILIENT provides assurance that the TOE agent is able to protect objects which compromise or affect its behavior by mediating all user actions against TSF services and data.
T.EAVES A malicious user could eavesdrop on network traffic to gain unauthorized access to the TOE server.	O.DISTRIB The TOE server will provide the ability to manage the behavior of TOE agents using secure channels.	O.DISTRIB ensures that the TOE server is capable of protecting transmitted data to and from TOE agents through trusted channels using the FIPS 140-2 validated VSEC module to secure TSF data in transit.
	O.EAVES The TOE agent will leverage a FIPS 140-2 validated cryptographic module to secure the communication channels to and from itself.	O.EAVES provides reasonable assurance that TSF data transmitted between distributed TOE components will not be disclosed to an unauthorized party by leveraging the FIPS 140-2 validated VSEC module for symmetric encryption.

Threats	Objectives	Rationale
T.FALSIFY A malicious user can falsify the identity of a TOE agent, providing the administrator with false assurance that the TOE is enforcing a policy.	OE.CRYPTO The TOE environment must be able to provide FIPS 140-2 validated cryptography to protect communications between the TOE server and TOE agent over insecure networks.	OE.CRYPTO ensures that the TOE server is able to leverage third party FIPS 140-2 validated modules to confirm its identity to TOE agents, and vice versa, while transmitting policy updates and bundle data.
T.FORGE A malicious user may create a false policy and send it to the TOE agent for consumption, adversely affecting its access control policy enforcement behavior.	OE.CRYPTO The TOE environment must be able to provide FIPS 140-2 validated cryptography to protect communications between the TOE server and TOE agent over insecure networks.	OE.CRYPTO ensures that the TOE server is able to leverage the third party FIPS 140-2 validated cryptographic providers to confirm its identity to TOE agents, and vice versa, while transmitting policy updates and bundle data to ensure that TSF data originates from a trusted source. By digitally signing and verifying policy and bundle data, the TOE is able to recognize and discard invalid or malicious input requests by users. It also ensures that the TOE is able to verify the integrity of transferred data between the TOE server and agent using secure hash algorithms and keyed message authentication codes.
T.UNATTEND A TOE server administrator may leave an authenticated session unattended, resulting in the possibility of a malicious or unauthorized user to mask their actions as the logged in user, resulting in a misconfiguration or alteration of the TSF behavior.	O.INACTIVE The TOE server must implement a robust mechanism for terminating user sessions after a period of inactivity.	O.INACTIVE ensures that the TOE server is capable of terminating user sessions after a configurable time interval.
T.MASQUERADE A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.AUTH The TOE server will provide a mechanism to examine user identity and credential data supplied by a user and compare it with the information stored in its database to determine the extent to which the claimed identity should be able to perform TSF management functions.	By ensuring that the TOE server is able to identify and authenticate users prior to allowing access to TOE administrative functions and data, O.AUTH satisfies this threat.
T.NODETECT An administrative user or end-user's actions may go undetected or be incorrectly recorded,	O.MONITOR The TOE server and TOE agents will monitor the behavior of themselves for anomalous activity.	O.MONITOR ensures that the TOE will monitor the behavior of itself for anomalous activity by generating security relevant

Threats	Objectives	Rationale
resulting in a failure to identify a potential security breach.		events that detect access attempts to TOE-protected resources by administrative users and end-users.
T.NOROUTE A malicious user may disrupt the internal communications between TOE server and TOE agent, adversely affecting access control behavior.	O.MAINTAIN The TOE agent will be capable of maintaining policy enforcement even if disconnected from the TOE server.	O.MAINTAIN ensures that the TOE is capable of enforcing access control policies in the event of a communications failure between the TOE server and TOE agents.
T.TAMPERING A user or process may be able to bypass the TOE agent's security mechanisms by tampering with the TOE server, TOE agent, or TOE environment.	O.ADMIN The TOE server and TOE agent must include a set of functions that allow efficient management of their functions and data, ensuring that TOE users with the appropriate privileges and/or secrets, and only those TOE users, may exercise such control.	O.ADMIN supports the mitigation of this threat by ensuring that only authorized users may configure the TOE server and TOE agent security mechanisms.
	OE.ENDUSERS The TOE environment shall restrict end-users of the TSF-mediated workstations to limited or non-administrative privileges.	OE.ENDUSERS ensures that users are restricted from performing administrative functions that may modify the behavior of the TSF.
	O.AUDIT The TOE agent will provide measures for generating security relevant events upon detecting access attempts to TSF-mediated resources in the TOE Environment, and the TOE server provides a mechanism through which the events can be reviewed by authorized administrators. The TOE server must also record events for operations performed through its management interfaces, as well as any relevant details, including outcome.	The objective O.AUDIT ensures that security relevant events that may indicate attempts to tamper with the TOE server or TOE agent are recorded.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering. To ensure this, operating systems on which the TOE software is installed must be appropriately secured following best practices guidance, and that all high-level security risks have been mitigated. This might	OE.PROTECT ensures that the TOE is protected from external interference or tampering.

Threats	Objectives	Rationale
	include installing anti-virus software on the operating systems which support the TOE, as well as placement of firewalls and intrusion detection sensors in the appropriate network locations.	
	O.PROTECT The TOE server must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	O.PROTECT mitigates this threat by providing mechanisms to protect the TSF data from unauthorized modification.
	O.RESILIENT The TOE agent must prevent users in the Operational Environment from performing actions that would disable or otherwise modify its behavior.	O.RESILIENT ensures that the TOE agent is capable of preventing TSF resources in the TOE environment from being tampered with or modified, and preventing itself from being disabled or terminated.
T.UNAUTH A user may bypass the TOE server's identification, authentication, or authorization mechanisms in order to illicitly utilize the TOE's management functions.	O.ADMIN The TOE server and TOE agent must include a set of functions that allow efficient management of their functions and data, ensuring that TOE users with the appropriate privileges and/or secrets, and only those TOE users, may exercise such control.	The objective O.ADMIN ensures that access to TOE security data is limited to those users with access to the management functions of the TOE server.
	O.AUDIT The TOE agent will provide measures for generating security relevant events upon detecting access attempts to TSF-mediated resources in the TOE Environment, and the TOE server provides a mechanism through which the events can be reviewed by authorized administrators. The TOE server must also record events for operations performed through its management interfaces, as well as any relevant details, including outcome.	The objective O.AUDIT ensures that unauthorized attempts to access the TOE or TSF-mediated resources are recorded.
	O.AUTH The TOE server will provide a mechanism to examine user identity and credential data supplied by a user and compare it with the information stored in its database to determine the extent	The objective O.AUTH ensures that users are identified and authenticated prior to gaining access to TOE server functions.

Threats	Objectives	Rationale
	to which the claimed identity should be able to perform TSF management functions.	
T.UNAUTH2 A malicious or careless user may access an object in the TOE environment that causes disclosure of sensitive or proprietary data, or adversely affects the behavior of a system.	O.DATAPROT The TOE agent will protect sensitive user data from unauthorized access, modification, loss, or disclosure by enforcing an access control policy produced by the TOE server, and by performing classification and encryption of data according to a set of sensitivity criteria. The TOE server must ensure that only authorized administrators possess the ability to configure policies to be enforced by the TOE agent.	O.DATAPROT mitigates this threat by ensuring that the TOE agent enforces access control appropriately on sensitive user data to prevent loss or disclosure, and that the policies enforced are maintained by the TOE administrator.
T.WEAKPOL A policy administrator may be incapable of using the TOE server to define policies in sufficient detail to facilitate robust access control, causing the TOE agent's access control mechanism to behave in a manner that allows illegitimate activity or prohibits legitimate activity.	OE.ENDUSERS The TOE environment shall restrict end-users of the TSF-mediated workstations to limited or non-administrative privileges.	OE.ENDUSERS ensures that users are prevented from observing the TOE and thus identifying weak enforcement policies.
	NOE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	NOE.MANAGE ensures that the individuals designated as policy administrators are carefully selected, and properly trained.
T.UNOBSERV A malicious or careless end-user may instigate a high-risk security event or policy, which may go unnoticed by the TOE operators responsible for enforcing the organizational security policy.	O.NOTIFY The TOE server must possess the capability of detecting policy violations and alerting the appropriate personnel when such anomalous activity occurs.	O.NOTIFY provides assurance that the TOE server is capable of detecting violations and alerting the appropriate personnel by sending email notifications.
	O.REVIEW The TOE server must provide a mechanism to identify access control policy violations and to provide tools necessary to view and respond to violations by authorized TOE operators.	O.REVIEW provides assurance that the TOE server provides the tools necessary to review and respond to policy violations.
T.WEAKCIPHERS A TOE administrator may improperly configure the TOE to use weak ciphers and key sizes, thus compromising the TOE's ability to protect user data.	O.STRONGCRYPTO The TOE agent must implement a FIPS 140-2 validated cryptographic module leveraging secure approved algorithms to protect sensitive data and CSPs from	O.STRONGCRYPTO ensures that all cryptographic functionality provided by the TOE agent has been FIPS 140-2 validated.

Threats	Objectives	Rationale
	modification or disclosure.	

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

8.2.2 Security Objectives Rationale Relating to Policies

Table 26 below gives a mapping of policies and the objectives that support them.

Table 26 - Policies:Objectives Mapping

Policies	Objectives	Rationale
P.MANAGE The TOE server and TOE agent may only be managed by authorized users.	O.ADMIN The TOE server and TOE agent must include a set of functions that allow efficient management of their functions and data, ensuring that TOE users with the appropriate privileges and/or secrets, and only those TOE users, may exercise such control.	O.ADMIN ensures that the TOE server and TOE agent provide the necessary tools to support the P.MANAGE policy.
	O.AUTH The TOE server will provide a mechanism to examine user identity and credential data supplied by a user and compare it with the information stored in its database to determine the extent to which the claimed identity should be able to perform TSF management functions.	O.AUTH ensures that only authorized users are granted access to the tools required to manage the TOE.
P.INTEGRITY Data collected and produced by the TOE server and TOE agents must be protected from modification.	O.ADMIN The TOE server and TOE agent must include a set of functions that allow efficient management of their functions and data, ensuring that TOE users with the appropriate privileges and/or secrets, and only those TOE users, may exercise such control.	O.ADMIN ensures that the TOE server and TOE agent only permit authorized users to exercise their management functions.
	O.PROTECT The TOE server must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	O.PROTECT ensures that the TOE server protects audit and system data to meet this policy.
P.BANNER The TOE server shall display an initial banner describing restrictions of use, legal	O.BANNER The TOE server will display an advisory warning regarding use of the TOE.	O.BANNER ensures that an advisory warning is displayed regarding the use of the TOE.

Policies	Objectives	Rationale
agreements, or any other appropriate information to which users consent by accessing the system.		
P.UPDATEPOL The organization will exercise due diligence to ensure that the TOE is updated with relevant policy data.	O.POLICY The TOE server will provide capabilities for managing policies that the TOE agents will enforce, based on a set of rules containing subject and object attributes.	O.POLICY ensures that the TOE server provides administrators with the tools necessary to keep TOE agents updated with the most recent policies.

Every policy is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives enforce all defined policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 27 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 27 - Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.AUTHENTICATE Subjects acting as end-users of the TOE agent are authenticated by a secure mechanism in the TOE environment that works in conjunction with the repository responsible for maintaining user identity and attribute data.	OE.USERID The TOE environment must be able to identify the user requesting access to TSF-mediated resources and convey validation of this to the TOE.	OE.USERID satisfies this assumption by ensuring the existence of a mechanism which validates user login attempts on TOE agent-mediated computers against a repository of user identity and credential attributes.
A.ENDUSERS End-users of the TOE are assumed to posess a low-skill level with little to no knowledge of the TOE, and are not afforded local administrator rights on TOE agent-mediated machines.	OE.ENDUSERS The TOE environment shall restrict end-users of the TSF-mediated workstations to limited or non-administrative privileges.	OE.ENDUSERS satisfies this assumption by restricting end-users of TSF-mediated workstations to limited or non-administrative privileges.
A.INSTALL The TOE is installed on the appropriate, dedicated hardware and operating system necessary to support the error-free operation of the TSF.	OE.PLATFORM The TOE hardware and OS must support all required TOE functions.	OE.PLATFORM ensures that the TOE hardware and OS supports the TOE functions.
A.LOCATE The TOE server is located within a controlled access facility.	NOE.PHYSICAL The physical TOE server environment must be suitable for supporting a computing device in a secure setting and must provide adequate physical security to prevent unauthorized access or tampering.	Physical security is provided within the TOE server environment to provide appropriate protection to the network resources. NOE.PHYSICAL satisfies this assumption.

Assumptions	Objectives	Rationale
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.ADMIN There will be one or more administrators of the TOE environment that will be responsible for providing subject identity to attribute mappings within the TOE.	OE.ADMIN provides assurance that the organization has assigned a responsible person for managing user identity and attribute data used within the TOE.
	NOE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	Those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use. NOE.MANAGE satisfies this assumption.
A.NETCON The TOE environment provides the network connectivity required to allow distributed TOE components to communicate.	OE.NETWORK The TOE environment must consist of a dedicated, secure network, to which distributed TOE components will be attached, along with other services necessary to support the TSF, such as a central repository for supplying user and computer identity information.	OE.NETWORK satisfies the assumption that the TOE environment will provide the appropriate connectivity to allow the TOE to perform its function.
A.NOEVIL The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	NOE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	NOE.MANAGE satisfies the assumption that the users who manage the TOE are non-hostile, appropriately trained and follow all guidance.
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering. To ensure this, operating systems on which the TOE software is installed must be appropriately secured following best practices guidance, and that all high-level security risks have been mitigated. This might include installing anti-virus software on the operating systems which support the TOE, as well as placement of firewalls and intrusion detection sensors in the appropriate network locations.	The TOE environment provides protection from external interference or tampering. OE.PROTECT satisfies this assumption.

Assumptions	Objectives	Rationale
A.SECURECOMM Because the TOE's distributed components (server and agent) may not be located within the same controlled access facility or connected to the same protected physical network, it is assumed that the IT environment will provide a secure line of communication between the TOE server and agent and between the TOE server and remote administrators.	OE.CRYPTO The TOE environment must be able to provide FIPS 140-2 validated cryptography to protect communications between the TOE server and TOE agent over insecure networks.	By leveraging the 3rd party FIPS 140-2 validated cryptographic modules in the TOE environment, the OE.SECURECOMM objective satisfies this assumption.
A.TIMESTAMP The IT environment provides the TOE server and TOE agent with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME satisfies the assumption that the environment provides reliable timestamps to the TOE.
A.USERID Identity and attribute data for TOE agent users is provided by a secure organizational repository in the TOE environment.	OE.NETWORK The TOE environment must consist of a dedicated, secure network, to which distributed TOE components will be attached, along with other services necessary to support the TSF, such as a central repository for supplying user and computer identity information.	OE.NETWORK satisfies this assumption by ensuring that a centralized repository of user identity and credential information by which end-users are validated is available to the TOE.
	OE.USERID The TOE environment must be able to identify the user requesting access to TSF-mediated resources and convey validation of this to the TOE.	OE.USERID satisfies this assumption by requiring the TOE environment to supply a reliable mechanism for validating user identification and authentication requests using security attribute data that is stored in a secure, centralized location.

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

8.3 Rationale for Extended Security Functional Requirements

Several families of ESM requirements were created to specifically address the lack of support for describing part of the security functionality exhibited by the TOE, such as association of security attributes with objects in the TOE environment, definition and transmission of access control policies between policy management and access control products, and discovering objects in the TOE environment to be classified, encrypted, or otherwise acted upon as a result of discovery. The FDP_ACC, FDP_IFC, FAU_ARP, FIA_ATD, and FIA_USB families were used as models for creating the extended ESM families. These requirements have no dependencies since the stated requirements embody all the necessary security

functions. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

Several families were added to the FAU class of requirements to address the need for describing audit functionality not specifically related to the operations performed on the TOE itself; rather they address those events occurring in the TOE environment that the TSF is intended to mediate. The functionality of these families include event data generation, security violation analysis and alerting, and event data review/reporting. Existing families from the FAU class were used as models for creating these requirements. The functionality exhibited by these requirements can easily be documented in the ADV and thus do not require any additional Assurance Documentation.

8.4 Rationale for Extended TOE Security Assurance Requirements

No extended Security Assurance Requirements are defined for this Security Target.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 28 below shows a mapping of the objectives and the SFRs that support them.

Table 28 - Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE server and TOE agent must include a set of functions that allow efficient management of their functions and data, ensuring that TOE users with the appropriate privileges and/or secrets, and only those TOE users, may exercise such control.	FDP_ACC.1(1) Subset access control (TOE server)	The SFR meets the objective by enforcing the Management Access Control SFP to determine the actions which can be performed by management users.
	FDP_ACF.1(1) Security attribute based access control (TOE server)	The SFR meets the objective by enforcing the Management Access Control SFP to determine the actions which can be performed by management users based on the privilege levels contained in their assigned roles.
	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE server and TOE agent restrict operations resulting in a modification of the TSF to a set of authorized roles, thus ensuring that administrative functions are only available to those users with the appropriate privileges, and/or those who possess secrets used to disable the TOE agent.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE server and TOE agent include administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE server associates users with roles to provide access to TSF management functions and data.
O.AUDIT The TOE agent will provide measures for generating security relevant events upon detecting	FAU_GEN.1(1) Audit data generation (TOE server)	This SFR requires that the TOE server record security-relevant operations performed through its management console. It also

Objective	Requirements Addressing the Objective	Rationale
access attempts to TSF-mediated resources in the TOE Environment, and the TOE server provides a mechanism through which the events can be reviewed by authorized administrators. The TOE server must also record events for operations performed through its management interfaces, as well as any relevant details, including outcome.		ensures that each event log contains necessary details associated with the event, thus satisfying the objective.
	FAU_GEN.1(2) Audit data generation (TOE agent)	This SFR requires that the TOE agents record forensic activity occurring in the TSF-mediated environment to be sent to the TOE server for further analysis and review. It also ensures that each event log contains necessary details associated with the event, thus satisfying the objective.
	FAU_SAR.1(1) Audit review (TOE server data)	This SFR requires that the audit data generated by the TOE server as a result of operations performed through its management console is provided to TOE administrators in a human-interpretable format for review, thus satisfying the objective.
	FAU_SAR.1(2) Audit review (TOE agent data)	The requirement meets the objective by ensure that the TOE server provides the ability to review logs containing forensic activity within the TSF-mediated environment. This functionality is provided by the DGMC for authorized users.
O.AUTH The TOE server will provide a mechanism to examine user identity and credential data supplied by a user and compare it with the information stored in its database to determine the extent to which the claimed identity should be able to perform TSF management functions.	FDP_ACC.1(1) Subset access control (TOE server)	The SFR meets the objective by enforcing the Management Access Control SFP which is is to determine the user's authorized functions.
	FDP_ACF.1(1) Security attribute based access control (TOE server)	The SFR meets the objective by enforcing the Management Access Control SFP based on the privilege levels associated with the user's role. These privilege levels are used to determine the authorized actions for that user.
	FIA_UAU.2 User authentication before any action	This SFR requires the TOE server to only allow properly authenticated users to perform any actions through the DGMC, thus satisfying the objective.
	FIA_UID.2	This SFR requires the TOE server

Objective	Requirements Addressing the Objective	Rationale
	User identification before any action	to only allow properly identified users to perform any actions through the DGMC, thus satisfying the objective.
	FMT_MOF.1 Management of security functions behaviour	The SFR meets the objective by requiring the TOE server to use its authorization mechanism to determine the administrative functions allowed for identified and authenticated users, ensuring that only those trusted users may manage the security behaviour of the TOE.
	FMT_MSA.1 Management of security attributes	To ensure that only the appropriately authorized users are permitted access to TOE server management functions, the SFR requires that the TOE server's authorization mechanism analyzes a set of user security attributes to determine the actions for which the user should be granted access, thus satisfying the objective.
	FMT_MSA.3 Static attribute initialisation	This SFR ensurs that attributes used to determine the extent to which users are authorized to perform management functions are given secure default values.
	FMT_SMR.1 Security roles	To provide a clear separation of administrative tasks, and to ensure that appropriately authorized roles are restricted to specific administrative functions, this SFR requires the TOE server to use the user's role information to determine the actions to be allowed, thus satisfying the objective.
O.BANNER The TOE server will display an advisory warning regarding use of the TOE.	FTA_TAB.1 Default TOE access banners	This requirement ensures that a banner is displayed to end-users of the DGMC prior to identification and authentication, thus satisfying the objective.
O.DATAPROT The TOE agent will protect sensitive user data from unauthorized access, modification, loss, or disclosure by enforcing an	ESM_DSC_EXT.1 Object discovery	The SFR meets the objective by using the TOE agent to classify objects at rest that are found to meet a set of sensitivity criteria according to the Enterprise

Objective	Requirements Addressing the Objective	Rationale
access control policy produced by the TOE server, and by performing classification and encryption of data according to a set of sensitivity criteria. The TOE server must ensure that only authorized administrators possess the ability to configure policies to be enforced by the TOE agent.		Information Protection SFP, and performing an action (encryption, classification, user prompt, etc.) upon triggering of the rule contained within a policy.
	FCS_COP.1 Cryptographic operation	The SFR meets this objective by requiring the TOE agent to encrypt sensitive files and/or entire storage volumes deemed by an administrator as necessary, to ensure that all sensitive data is protected from unauthorized disclosure.
	FDP_ACC.1(2) Subset access control (TOE agent)	The SFR meets the objective by preventing end-users from accessing or transmitting sensitive data which is disallowed by the Enterprise Information Protection SFP, which is enforced on TOE agents using policies received from the TOE server.
	FDP_ACF.1(2) Security attribute based access control (TOE agent)	The SFR meets the objective by enforcing the Enterprise Information Protection SFP on the TOE agent based on rules composed of subject and object attributes, which are used to determine the allowed operations for a subject acting upon an object in the TOE environment.
	FDP_ITC.1 Import of user data without security attributes	The TOE provides administrators during installation the ability to import cryptographic keys to be used by the TOE agents to encrypt and decrypt sensitive data, thus satisfying the objective.
	FMT_MOF.1 Management of security functions behaviour	The SFR meets the objective by restricting the ability to manage access control policies through the TOE server to an authorized TOE administrator.
	FMT_SMF.1 Specification of management functions	In order to enforce an access control policy, the TOE server must provide the ability for such a policy to be configured. The SFR meets the objective by providing a mechanism (DGMC) through which access control policies can

Objective	Requirements Addressing the Objective	Rationale
		be managed.
O.DISTRIB The TOE server will provide the ability to manage the behavior of TOE agents using secure channels.	ESM_ACT_EXT.1 Access control policy transmission	This requirement ensures that access control policies are distributed in a manner that ensures the most up to date policy to be enforced at the TOE agent, thus satisfying the objective.
	FPT_ITT.1 Basic internal TSF data transfer protection	Using the cryptographic support provided by the VSEC module, the TOE will use symmetric encryption to provide a secure channel used to protect TSF data transmitted between the TOE server and TOE agents, thus satisfying the objective.
O.EAVES The TOE agent will leverage a FIPS 140-2 validated cryptographic module to secure the communication channels to and from itself.	FPT_ITT.1 Basic internal TSF data transfer protection	Using the cryptographic support provided by the VSEC module, this SFR provides reasonable assurance that TSF data cannot be disclosed to an unauthorized party, thus satisfying the objective.
O.INACTIVE The TOE server must implement a robust mechanism for terminating user sessions after a period of inactivity.	FTA_SSL.3 TSF-initiated termination	To mitigate the risk of unauthorized users gaining access to unattended sessions, this SFR requires the TOE server to enforce session validity on a per request basis, ensuring that no activity can be performed on stale sessions once an inactivity threshold has been reached.
O.MAINTAIN The TOE agent will be capable of maintaining policy enforcement even if disconnected from the TOE server.	FPT_FLS.1 Failure with preservation of secure state	The SFR meets the objective by requiring that the access control capabilities of the TOE agent maintain resiliency by continuing to enforce the most recently applied policy in the event of a communications failure with the TOE server, and immediately upon re-establishment of communication, apply the most recently published policy to ensure that any changes to the policy during an outage are applied as early as possible.
	FRU_FLT.1 Degraded fault tolerance	The SFR satisfies the objective by requiring that the access control enforcement capabilities of the TOE agent are resumed during a

Objective	Requirements Addressing the Objective	Rationale
		loss of communication with the TOE server, and as a result are able to thwart an attempt to disrupt TSF enforcement by breaking the communications link.
O.MONITOR The TOE server and TOE agents will monitor the behavior of themselves for anomalous activity.	FAU_GEN.1(1) Audit data generation (TOE server)	The SFR ensures that the TOE server is capable of generating audit information to prevent malicious users from masking their actions, and that any activity intended to sabotage or misconfigure the TOE through its management interfaces is recorded, thus satisfying the objectvice.
	FAU_GEN.1(2) Audit data generation (TOE agent)	The SFR requires that all actions performed on TSF-mediated resources in the TOE environment are recorded, including any TOE agent failures, in an effort to prevent malicious activity from being masked or undetected, thus satisfying the objective.
O.NOTIFY The TOE server must possess the capability of detecting policy violations and alerting the appropriate personnel when such anomalous activity occurs.	FAU_ARP.1 Security alarms	To mitigate the risk of policy violations that go undetected or unreviewed, this SFR requires the TOE server to send a notification to administrators when an access control rule to which they are subscribed has been triggered, thus satisfying the objective.
	FAU_SAA.1 Potential violation analysis	In order to detect anomalous behavior, the TOE server must have a mechanism for detecting violations of enforced policy, which this SFR aims to enforce, thus satisfying the objective.
O.POLICY The TOE server will provide capabilities for managing policies that the TOE agents will enforce, based on a set of rules containing subject and object attributes.	ESM_ACD_EXT.1 Access control policy definition	The SFR meets the objective by requiring the TOE server to provide methods for creating, modifying, deleting, and assigning policies.
	ESM_OAD_EXT.1 Object attribute definition	This SFR requires the TOE server to maintain a set of attributes for objects in the TOE environment, which are used to determine the actions to be performed by the

Objective	Requirements Addressing the Objective	Rationale
		TOE agents, thus satisfying the objective.
	FMT_MSA.1 Management of security attributes	This SFR requires that the TOE server is able to define policies using a set of secure attributes which are used to determine the access control behavior of the agents in which the policies are intended to be enforced, thus satisfying the objective.
	FMT_MSA.3 Static attribute initialisation	This SFR meets the objective by requiring the TOE to supply permissive defaults when defining a policy, as well as an ability to override the default behavior.
	FMT_SMF.1 Specification of management functions	This SFR specifies the management functions involved in creating, deleting, modifying, and assigning policies, thus satisfying the objective.
O.PROTECT The TOE server must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that the TOE server protects itself from unauthorized modification. The TOE server does this by ensuring that only authenticated users are allowed access to TOE functions.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the TOE server protects itself from unauthorized modification. The TOE server does this by ensuring that only identified users are allowed access to TOE management functions.
	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE server protects itself from unauthorized modification. The TOE server does this by ensuring that only privileged users may perform a set of operations resulitng in modification of the security behaviour of the TOE based on a set of authorized roles.
O.RESILIENT The TOE agent must prevent users in the Operational Environment	FMT_MOF.1 Management of security functions behaviour	The TOE agent ensures that end-users of the TOE environment cannot observe, tamper with,

Objective	Requirements Addressing the Objective	Rationale
from performing actions that would disable or otherwise modify its behavior.		disable, or otherwise modify its behavior unless they possess the necessary tools and site-secrets.
O.STRONGCRYPTO The TOE agent must implement a FIPS 140-2 validated cryptographic module leveraging secure approved algorithms to protect sensitive data and CSPs from modification or disclosure.	FCS_CKM.1 Cryptographic key generation	To prevent the use of unapproved key generation techniques, this SFR requires that a FIPS 140-2 validated module is implemented to generate symmetric encryption keys, thus satisfying the objective.
	FCS_CKM.4 Cryptographic key destruction	To prevent re-use or disclosure of sensitive CSPs, this SFR requires that all keys are zeroized from volatile memory when they are no longer in use, thus satisfying the objective.
	FCS_COP.1 Cryptographic operation	To prevent the use of weak ciphers, this SFR requires that a FIPS 140-2 validated module is implemented to encrypt, decrypt, sign, hash, and authenticate sensitive data using approved algorithms, thus satisfying the objective.
O.REVIEW The TOE server must provide a mechanism to identify access control policy violations and to provide tools necessary to view and respond to violations by authorized TOE operators.	FAU_SAR.1(2) Audit review (TOE agent data)	This SFR requires that the TOE server is able to provide authorized administrators with a mechanism for reviewing TOE agent event data and responding to access control violations, thus satisfying the objective.

8.5.2 Security Assurance Requirements Rationale

EAL2+ was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment. The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 29 lists each requirement to which the TOE claims

conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 29 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
ESM_ACD_EXT.1	No dependencies	✓	
ESM_ACT_EXT.1	ESM_ACD_EXT.1	✓	
ESM_DSC_EXT.1	No dependencies	✓	
ESM_OAD_EXT.1	No dependencies	✓	
FAU_ARP.1	FAU_SAA.1	✓	
FAU_GEN.1(1)	FPT_STM.1	✓	OE.TIME ensures that timestamps are provided by the Operating Environment, therefore this dependency is met.
FAU_GEN.1(2)	FPT_STM.1	✓	OE.TIME ensures that timestamps are provided by the Operating Environment, therefore this dependency is met.
FAU_SAA.1	FAU_GEN.1(2)	✓	
FAU_SAR.1(1)	FAU_GEN.1(1)	✓	
FAU_SAR.1(2)	FAU_GEN.1(2)	✓	
FCS_CKM.1	FCS_CKM.4	✓	
	FCS_COP.1	✓	
FCS_CKM.4	FDP_ITC.1	✓	
FCS_COP.1	FCS_CKM.4	✓	
	FDP_ITC.1	✓	
FDP_ACC.1(1)	FDP_ACF.1(1)	✓	
FDP_ACC.1(2)	FDP_ACF.1(2)	✓	
FDP_ACF.1(1)	FDP_ACC.1(1)	✓	
	FMT_MSA.3	✓	
FDP_ACF.1(2)	FMT_MSA.3	✓	
	FDP_ACC.1(2)	✓	
FDP_ITC.1	FMT_MSA.3	✓	
	FDP_ACC.1(1)	✓	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included.

SFR ID	Dependencies	Dependency Met	Rationale
			This satisfies this dependency.
FIA_UID.2	No dependencies	✓	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
	FDP_ACC.1(1)	✓	
FMT_MSA.3	FMT_SMR.1	✓	
	FMT_MSA.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FPT_FLS.1	No dependencies	✓	
FRU_FLT.1	FPT_FLS.1	✓	
FTA_SSL.3	No dependencies	✓	
FTA_TAB.1	No dependencies	✓	
FPT_ITT.1	No dependencies	✓	

9 Acronyms

This section and Table 30 define the acronyms used throughout this document.

9.1 Acronyms

Table 30 - Acronyms

Acronym	Definition
ACM	Application Compliance
ACI	Adaptive Content Inspection
ADE	Application Data Exchange
ADI	Adaptive Data Inspection
AES	Advanced Encryption Standard
AFE	Adaptive File Encryption
AME	Adaptive Mail Encryption
API	Application Programming Interface
APT	Advanced Persistent Threat
CBC	Cipher Block Chaining
CC	Common Criteria
CD	Compact Disc
CEM	Common Evaluation Methodology
CM	Configuration Management
CPU	Central Processing Unit
CTR	Counter
DG	Digital Guardian
DGMC	Digital Guardian Management Console
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DTM	Documentum
DVD	Digital Versatile Disc
EAL	Evaluation Assurance Level
ECB	Electronic Codebook
EIP	Enterprise Information Protection
ESM	Enterprise Security Management
ETL	Extract, Transform, Load

Acronym	Definition
FIPS	Federal Information Processing Standard
GB	Gigabyte
GHz	Gigahertz
HMAC	Hash-based Message Authentication Code
ID	Identification
IIS	Internet Information Services
IM	Investigation Module
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
MB	Megabyte
NIST	National Institute of Standards and Technology
OS	Operating System
OSP	Organizational Security Policy
PII	Personally Identifiable Information
PKCS1	Public Key Cryptography Standard #1
PKI	Public Key Infrastructure
PP	Protection Profile
PUB	Publication
RAM	Random Access Memory
RME	Removable Media Encryption
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman
RSASSA	RSA Signature Scheme with Appendix
RSAENH	RSA Enhanced Cryptographic Provider
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SP	Service Pack
SPD	Security Problem Description

Acronym	Definition
SPT	SharePoint
SQL	Structured Query Language
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
UC	User Classification
USB	Universal Serial Bus
VPN	Virtual Private Network
VSEC	Verdasys Secure Cryptographic Module

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway
Suite 220
Fairfax, VA 22033

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com