eVault Technologies Sdn. Bhd.

SecureMi®
Version 1.2

Security Target
0.13

4 July 2017

DOCUMENT HISTORY

Version Number	Version Date	Change Details
0.1	14 March 2014	Fresh version
0.2	21 March 2014	Update base on comments from ADV_FSP table v0.1
0.3	10 June 2015	Update based on new endpoint architecture
0.4	11 June 2015	Update based on comment from MySEF-3-EXE-E042-EOR1-d1 24MAR15
0.5	3 August 2015	Update based on comment from MySEF-3-EXE-E042-EOR2-d1 13JUL2015
0.6	20 September 2015	Minor update adding Data Protection List onto Physical Scope of the TOE
0.7	20 October 2015	Update based on comment from MySEF-3-EXE-E042-EOR3-d1 15 Oct 2015
0.8	13 January 2016	Update based on SecureMi CMC Service
0.9	16 November 2016	Update incident matrix
0.10	23 November 2016	Minor changes on information of supported file type
0.11	27 November 2016	Minor update on incident matrix
0.12	1 December 2016	Minor update on TOE SUMMARY SPECIFICATION (ASE_TSS)
0.13	4 July 2017	Minor update on section 4.2, 5.2 and 5.3

TABLE OF CONTENTS

LIST OF TABLES

1 DOCUMENT INTRODUCTION

1.1 DOCUMENT CONVENTIONS

The following conventions have been applied in this document:

Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: assignment, selection, and iteration.

- The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by ~~strikethrough of text~~.
- The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized text* in square brackets, [*selection value*].
- The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment value].
- The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration number).

1.2 TERMINOLOGY

Table 1 - Terminology

Acronym	Meaning
AES	Advanced Encryption Standard
API	Application Programming Interface
CC	Common Criteria
CMC	Centralized Management Console
COTS	Commercial Off The Shelf
DLP	Data Leakage Prevention
FIPS PUB	Federal Information Processing Standards Publication
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
IP	Internet Protocol
PP	Protection Profile
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunications Union

Acronym	Meaning
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
TSS	TOE Summary Specification
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
PP	Protection Profile
RFC	Request For Comments
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

1.3 REFERENCES

Common Criteria (informally referred to as “CCv3.1”):

- Common Criteria Part 1 Version 3.1 Revision 4
- Common Criteria Part 2 Version 3.1 Revision 4
- Common Criteria Part 3 Version 3.1 Revision 4
- Common Methodology for Information Technology Security Evaluation (CEM) version 3.1 Revision 4

1.4 DOCUMENT ORGANIZATION

This ST is organized into the following sections:

- Section 2 (ST Introduction (ASE_INT)) provides an overview of the TOE security functions and describes the physical and logical scope for the TOE
- Section 3 (Conformance claims (ASE_CCL)) provides the CC conformance claims for the ST and the TOE;
- Section 4 (Security problem definition (ASE_SPD)) describes the threats, organizational security policies, and assumptions that pertain to the TOE and the TOE environment.
- Section 5 (Objectives (ASE_OBJ)) identifies the security objectives that are satisfied by the TOE and the TOE environment.
- Section 6 (Extended components definition (ASE_ECD)) provides a definition for any extended SFRs or SARs claimed by the TOE;
- Section 7 (Security Requirements (ASE_REQ)) presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE
- Section 8 (Security requirements rationale)) provides a rationale for the selected SFRs and SARs; and
- Section 9 (TOE summary specification (ASE_TSS)) describes the security functions provided by the TOE to satisfy the security requirements and objectives.

2 ST INTRODUCTION (ASE_INT)

2.1 ST AND TOE REFERENCE

ST Title	SecureMi® Version 1.2 Security Target
ST Version	0.13 4 July 2017
TOE Identification	SecureMi® version 1.2
CC Identification	Common Criteria for Information Technology Security Evaluation, Version 3.1 Release 4
Assurance Level	EAL 2
ST Author	Sam Soo, Lester Soo, Jimmy Liew
Keyword(s)	Data Leakage Prevention, Data Loss Prevention, DLP, Common Criteria.

2.2 TOE OVERVIEW

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

The TOE (SecureMi®) is a content aware **Data Leakage Prevention (DLP**) solution that is designed as a complete solution for preventing data leakage problems in government and corporate environments from the start. It has the capabilities to detect and prevent any unauthorized use and transmission of confidential information of an organization by insiders. It consists of policies, procedures, and technical controls that will be defined by organization's team members on a centralized management framework. It is capable of classify, discover, monitor, and protect data in use, data in motion, and data at rest through detection procedure with content's pattern matching techniques. The TOE then takes actions based on pre-defined policies to protect the information from leakage and misuse.

2.2.1 Brief Description of the components of the TOE

There are 3 components within the SecureMi® DLP suite that provides this functionality: SecureMi® Centralized Management Console (CMC), SecureMi® Storage, and SecureMi® Endpoint.

The SecureMi® Storage and SecureMi® Endpoint are managed through the SecureMi® Centralized Management Console (CMC), a web application with a consistent user interface across all the products. The SecureMi® Storage and SecureMi® Endpoint can each be used independently, or integrated with one or both of the others, to provide the sensitive data protection required by our customers. However, in order for any one of the other products to work, the SecureMi® CMC must also be installed. This is because the SecureMi® CMC is necessary to provide administrative access to the other products, and without it, there would be no way to manage the other products.

The SecureMi® Storage and SecureMi® Endpoint products perform content analysis on documents and transmissions using a shared, policy-driven engine. Using these

policies, an enterprise can examine communications, track end user actions, and locate stored documents that contain sensitive content, scan and fingerprint documents to be used to identify unstructured data elsewhere and determine whether the action being taken on that content should be permitted. Sensitive content might include Personally Identifiable Information (PII), such as national identification number, Non-Public Personal Information (NPI), such as email addresses, or information protected by the Payment Card Industry (PCI) Data Security Standard, such as credit card information. DLP policies can define documents or transmissions as sensitive based on their content, sender, device, file type, or file size. TOE provides built-in, expert policies for immediate use. Authorized officers of the products can also build their own custom policies to identify sensitive content specific to their enterprise.

2.2.2 TOE Type

The TOE type is a Data Leakage Prevention (DLP) solution.

2.2.3 TOE Policies

Sensitive content is information the enterprise needs to be protected from loss or misuse. The TOE uses subsystem called SecureMi® Endpoint Super Agent to detect sensitive content. SecureMi® Endpoint Super Agent uses 4 methods (pattern matching techniques) for detecting sensitive content:

- Creating keyword or phrases list that match sensitivity criteria of the content to be detected.
- Creating expression or character patterns that match sensitivity criteria of the content to be detected.
- Creating fingerprints of specific sensitive documents. File type supported by the fingerprinting process are *.txt, *.doc, *.docx, *.xls, *.xlsx and *.pdf only.
- File attributes or characters such as file type.

These methods implement the detection or pattern matching technique rules of a policy. Detection or pattern logic can be created based on the above techniques. For example, a policy violation will be triggered on when [keyword list 1] AND [keyword list 2] OR [expression1] conditions are met.

In addition to detection rules, each DLP policy also implements product-specific rules that detect attributes that may or may not be allowed such as:

- protocol characteristics, such as SMTP,
- device characteristics, such as a device's name, USB flash drive information or printer name,
- Memory content

Policy actions are automatically performed by a DLP product when specified rules are matched. Possible policy actions include the following:

Resource channel \ Action	Log Action	Notify Action	Justify Action	Keep Evidence Action	Block Action
Data Discovery	Incident event will be logged	Incident event will be emailed	Not applicable.	If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the	If turn on, in the event of an incident, a block action quarantine file (provided that file was

	in the system for reporting if turn on.	to the preferred authorized officer group if turn on.		original file remains untouched.	not controlled by other process, otherwise that file will be unable to be deleted) by removing the original file from its location and keep secretly within TOE system in encrypted form. However, user can request an Unlock Code from the authorized officer to recover the quarantine files.
Removable Storage Data	Incident event will be logged in the system for reporting if turn on.	Incident event will be emailed to the preferred authorized officer group if turn on.	If turn on, in the event of an incident, a justify action causes a popup message to appear to the end-user, requiring the end-user to provide text justifying the attempted action.	If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched.	If turn on, in the event of an incident, a block action quarantine file (provided that file was not controlled by other process, otherwise that file will be unable to be deleted) by removing the original file from its location and keep secretly within TOE system in encrypted form. However, user can request an Unlock Code from the authorized officer to recover the quarantine files. A block action also eject the device (if it is not being controlled) eventually.
Removable Storage Device	Incident event will be logged in the system for reporting.	Incident event will be emailed to the preferred authorized officer group if turn on.	If turn on, in the event of an incident, a justify action causes a popup message to appear to the end-user, requiring the end-user to provide text justifying the attempte	Not applicable.	Eject the device (if it is not being controlled) if the device is not registered into the white list.

			d action.		
Email	Incident event will be logged in the system for reportin g if turn on.	Incident event will be emailed to the preferred authorize d officer group if turn on.	If turn on, in the event of an incident, a justify action causes a popup message to appear to the end-user, requiring the end-user to provide text justifying the attempte d action.	Attach file: If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched. Key in message: Not applicable Clipboard file drop: If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched.	Attach file: If turn on, in the event of an incident, a block action terminates the application. Key in message: If turn on, in the event of an incident, a block action terminates the application. Clipboard file drop: If turn on, in the event of an incident, a block action terminates the application.
Clipboard	Incident event will be logged in the system for reportin g if turn on.	Incident event will be emailed to the preferred authorize d officer group if turn on.	If turn on, in the event of an incident, a justify action causes a popup message to appear to the end-user, requiring the end-user to provide text justifying the attempte d action.	Not applicable.	If turn on, in the event of an incident, a block action erase the clipboard content.
Print Screen	Incident event will be logged in the system for reportin g fi turn on.	Not applicable .	If turn on, in the event of an incident, a justify action causes a popup message	Not applicable.	If turn on, in the event of an incident, a block action erase the clipboard content.

			to appear to the end-user, requiring the end-user to provide text justifying the attempted action.		
HTTP	Incident event will be logged in the system for reporting.	Incident event will be emailed to the preferred authorized officer group if turn on.	If turn on, in the event of an incident, a justify action causes a popup message to appear to the end-user, requiring the end-user to provide text justifying the attempted action.	Attach file: If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched. Key in message: Not applicable Clipboard file drop: If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched.	Not applicable.
FTP	Incident event will be logged in the system for reporting if turn on.	Incident event will be emailed to the preferred authorized officer group if turn on.	If turn on, in the event of an incident, a justify action causes a popup message to appear to the end-user, requiring the end-user to provide text justifying the attempted action.	Attach file: If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched. Key in message: Not applicable Clipboard file drop: If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched.	Not applicable.

<table>
<tr>
<td>Peer-to-peer</td>
<td>Incident event will be logged in the system for reporting if turn on.</td>
<td>Incident event will be emailed to the preferred authorized officer group if turn on.</td>
<td>Not applicable.</td>
<td>Attach file: If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched.
Key in message: Not applicable
Clipboard file drop: If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Instant Messaging</td>
<td>Incident event will be logged in the system for reporting if turn on.</td>
<td>Incident event will be emailed to the preferred authorized officer group if turn on.</td>
<td>Not applicable.</td>
<td>
<table>
<tr><td>Attach file</td><td>If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched.</td></tr>
<tr><td>Key in message</td><td>Not applicable</td></tr>
<tr><td>Clipboard file drop</td><td>If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched.</td></tr>
</table>
</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Printer</td>
<td>Incident event will be logged in the system for reportin</td>
<td>Incident event will be emailed to the preferred authorized officer</td>
<td>If turn on, in the event of an incident, a justify action causes a</td>
<td colspan="2">Not applicable.</td>
<td>If turn on, in the event of an incident, a block action delete the print job (if the length of time for the print job to print is long enough for the TOE to filter it).</td>
</tr>
</table>

	g if turn on.	group if turn on.	popup message to appear to the end-user, requiring the end-user to provide text justifying the attempte d action.		

Note: The TOE supports Unknown and Invalid File Type except for data discovery policy type. File types that are unable to extract text file (e.g. *.exe file) is defined as unknown file type. If user change a PDF file (says, abc.pdf) to different extension (says, abc.zip), system will defined this as invalid file type. Both unknown and invalid file type will trigger an incident. The TOE also disables the file drag and drop function.

Each policy action taken is captured in an event record, and passed to the SecureMi® CMC for viewing by the authorized officer.

2.2.4 Hardware, software and firmware required by the TOE

The essential components for the proper operation of the TOE in the evaluated configuration are:

- Customer provided hardware for SecureMi® CMC and SecureMi® Storage;
- Microsoft Internet Explorer 11 or Google Chrome 32 or Mozilla Firefox 27 web browser installed on the SECUREMI® CMC server, or optionally a management workstation from which the TOE will be managed. Please make sure your web browser supports HTML5 input types such as color, date, date/time and URL;
- Target customer workstations, servers and laptops on which SecureMi® Endpoint will be installed; and
- Oracle MySQL database to serve as CMC database.

Table 2 - TOE hardware/software requirements (below) lists the minimum hardware and software requirements for the TOE in the CC evaluated configuration:

Table 2 - TOE hardware/software requirements

Component	Hardware Requirements	Software Requirements
TOE		

Component	Hardware Requirements	Software Requirements
SecureMi® Centralized Management Console (CMC)	Server-class computer or Virtual hosting 2x 2.83 GHz or better CPU 4GB RAM 1 GB Storage	Supported OS: • 64-bit: Windows Server 2008 SP2, R2 • 32-bit: Windows Server 2008 SP2, R2 • 64-bit: Windows Server 2012 • 32-bit: Windows Server 2012 Evaluated OS: • 64-bit: Windows Server 2008 • 64-bit: Windows Server 2012 Evaluated Database: • Oracle MySQL 5.6 Evaluated Browsers: • Opera 41.0.2353.46 • Google Chrome 54.0.2840.71

Component	Hardware Requirements	Software Requirements
SecureMi® Storage	Server-class computer or Virtual hosting 2x 2.83 GHz or better CPU 4GB RAM 1 GB Storage	Supported OS: • 64-bit: Windows Server 2008 SP2, R2 • 32-bit: Windows Server 2008 SP2, R2 • 64-bit: Windows Server 2012 • 32-bit: Windows Server 2012 Evaluated OS: • 64-bit: Windows Server 2008 • 64-bit: Windows Server 2012 Evaluated Database: • Oracle MySQL 5.6 Perquisite: • .NET Framework 4.0 • Java version 8 update 111

Component	Hardware Requirements	Software Requirements
SecureMi® Endpoint	Workstation-class computer or virtual hosting 1GB RAM 300 MB Storage	Supported OS: 64-bit: • Windows Vista SP2 • Windows Server 2003 SP2 and R2 SP2 • Windows 7 Professional • Windows 7 Enterprise • Windows Server 2008 R2 and SP2 • Windows 8 Professional • Windows 10 Pro 32-bit: • Windows Vista SP2 • Windows Server 2003 SP2 and R2 SP2 • Windows 7 Professional • Windows 7 Enterprise • Windows Server 2008 R2 and SP2, • Windows 8 Professional • Windows 10 Pro Evaluated OS: • Windows 7 (32-bit) • Windows 8 (64-bit) • Windows 10 Pro (64-bit) Perquisite: • .NET Framework 4.0 • Java version 8 update 111
TOE Environment		

Component	Hardware Requirements	Software Requirements
SecureMi® CMC Database	Server-class computer or Virtual hosting 2x 2.83 GHz or better CPU 4GB RAM 1 GB Storage	Supported OS: • 64-bit: Windows Server 2008 SP2, R2 • 32-bit: Windows Server 2008 SP2, R2 • 64-bit: Windows Server 2012 • 32-bit: Windows Server 2012 Evaluated OS: • 64-bit: Windows Server 2008 • 64-bit: Windows Server 2012 Evaluated Database: Oracle MySQL 5.6
SecureMi® Endpoint Cache Database	Workstation-class computer or virtual hosting 1GB RAM 300 MB Storage	Evaluated OS: • Windows 7 (32-bit) • Windows 8 (64-bit) • Windows 10 Pro (64-bit) Evaluated Database: • Microsoft SQL CE 3.5

No firmware is needed by the TOE.

2.3 TOE DESCRIPTION

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

2.3.1 Physical scope of the TOE

The TOE is software that runs on customer-provided hardware compliant to the minimum software and hardware requirements as listed in Table 2. The TOE is installed in an enterprise network as depicted in the Figure 1. The essential components for the proper operation of the TOE in the evaluated configuration are:

- SecureMi® Centralized Management Console (CMC) v1.2 software
- SecureMi® Storage v1.2 software
- SecureMi® Endpoint v1.2 software
- SecureMi® Endpoint Service v1.2 software
- SecureMi® CMC Service v.1.2 software

Figure 1 – TOE boundary and subsystems below illustrates the subsystems and boundary of the TOE in logical view along with the environment in which it is used.

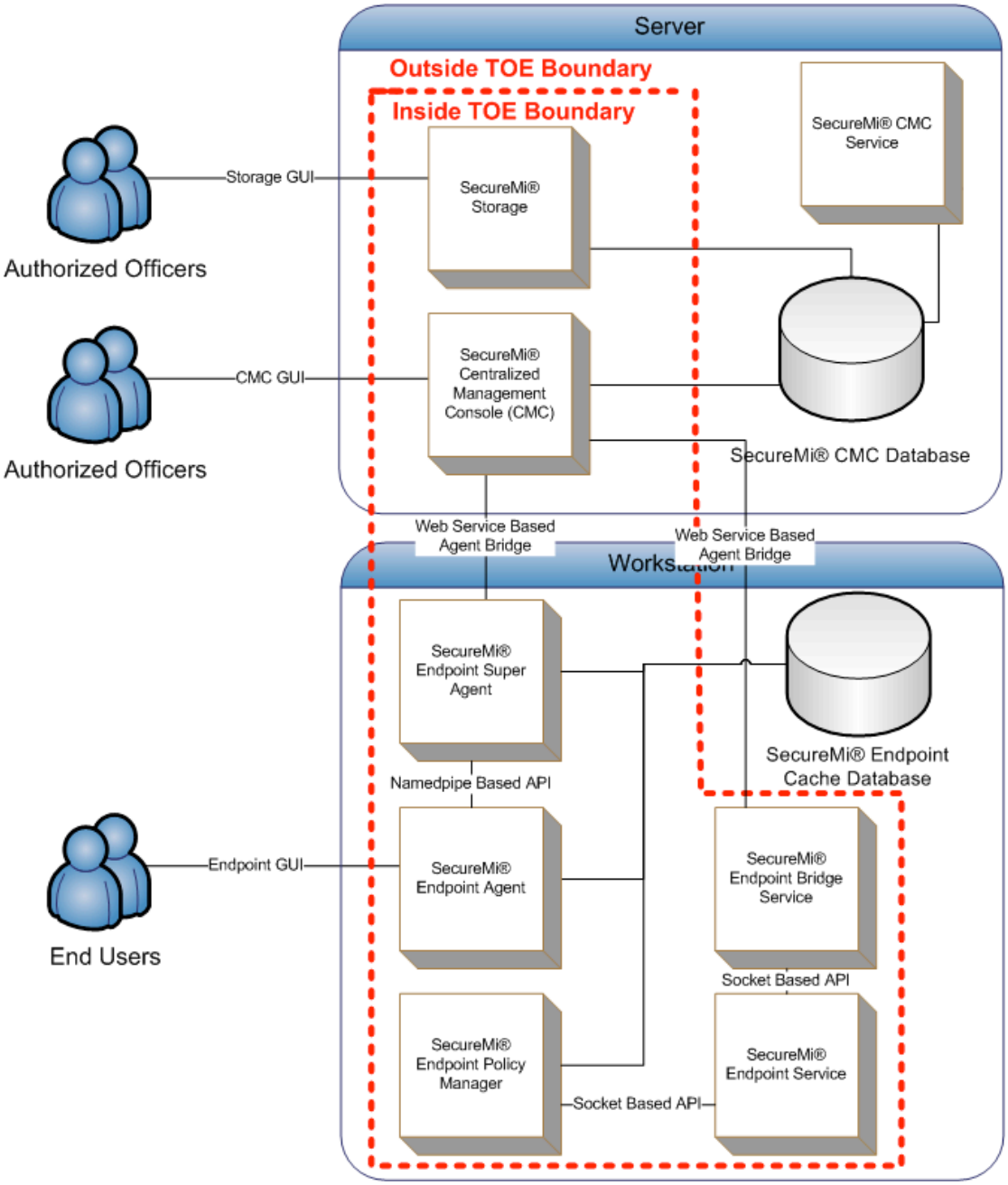

Figure 1 – TOE boundary and subsystems

There are three TOE components in a SecureMi®, namely:

- SecureMi® Centralized Management Console (CMC)
- SecureMi® Storage
- SecureMi® Endpoint

Although not part of the TOE, the following two parts of the environment perform services essential to the operation of the TOE:

- SecureMi® CMC Database
- SecureMi® Endpoint Cache Database

SecureMi® Centralized Management Console (CMC)

SecureMi® CMC is a web application with which an authorized officer configures and manages all the other DLP products. SecureMi® CMC is accessed through a standard web browser over HTTPS (CMC GUI). Each installation of DLP products typically includes only one instance of SecureMi® CMC. SecureMi® CMC requires a database, called the SecureMi® CMC Database, for storing the configurations, security policies, and the results of analyses performed by the other components.

Through the SecureMi® CMC, authorized officers can create, modify, delete and synchronize policies to an agent group, manage authorized officers, groups, and roles, customize notifications when a violation of security has been detected, update product licenses, generate one time password to unlock quarantine data in an endpoint agent, generate one time password to temporary switch off an endpoint agent, generate reports from events and incidents, and view DLP statistic. The SecureMi® CMC stores and retrieves data to and from the SecureMi® CMC Database.

In other words, SecureMi® CMC web application provides the interface into initialization and maintenance services, as well as the primary operator interface for day-to-day management of authorized officers following the assigned roles and their rights. It is the primary interface to the SecureMi® Endpoint Services. For every service offered there is at least one corresponding set of functions that enable operators to invoke that service.

SecureMi® CMC Service

SecureMi® CMC Service as one of SecureMi® CMC's module is a software agent that install on together with SecureMi® CMC on the same machine. It is software service that starts when the computer starts. This software is responsible to send out notification email to respective authorized officers and assists on the process of fingerprinting.

SecureMi® Storage

SecureMi® Storage is a software agent that install on together with SecureMi® CMC on the same machine. It is software service that starts when the computer starts and has a system tray icon on server and provides Graphical User Interface (Storage GUI) for authorized officer to retrieve quarantined documents from data discovery scanning. Authorized officer can enlist an unlimited number of files on SecureMi® CMC to be tag as sensitive data in the system. Once the source path and the schedule to scan were defined, SecureMi® Storage will automatically classify the files so that these fingerprints can be used to identify confidential data elsewhere.

SecureMi® Endpoint

SecureMi® Endpoint consists of five subsystems: SecureMi® Endpoint Super Agent, SecureMi® Endpoint Agent, SecureMi® Endpoint Policy Manager, SecureMi® Endpoint Service and SecureMi® Endpoint Bridge Service. The SecureMi® Endpoint Super Agent enforces policies on usage of data, resulting in blockages, justifications, or notifications, and generates events that describe the violations and the actions taken to enforce the policies.

SecureMi® Endpoint Policy Manager pushes these events and policy violated incidents to the SecureMi® CMC and also retrieves configuration settings and policy information from the SecureMi® CMC. SecureMi® Endpoint Agent displays as a system tray icon on end user's computer and provides Graphical User Interface (Endpoint GUI) for end user to retrieve quarantined documents, provides a vault to keep sensitive documents as well as provides policy violated messages and accept justification text from end-users.

SecureMi® Endpoint Bridge Service interacts with SecureMi® CMC to manage on SecureMi® Endpoint installation and patch updates and it will work together with SecureMi® Endpoint Service to accomplish this objective.

The SecureMi® Endpoint is software service that starts when the computer starts, and monitors end-user actions as long as the computer is running. SecureMi® Endpoint runs from within the targeted machine's operating system, and are transparent to desktop applications. The SecureMi® Endpoint injects itself into each running process on the targeted machine, and intercepts and monitors application calls. When an application call for an end-user action such as copy, move, or print is intercepted, the SecureMi® Endpoint extracts the content of the document involved, and performs an analysis on the content to determine if a policy violation has occurred. If so, the SecureMi® Endpoint performs the necessary actions based on the policy retrieve earlier from SecureMi® CMC.

Some audit, event and incident logs captured by SecureMi® Endpoint are stored temporary in the client side database namely SecureMi® Endpoint Cache Database (SQL CE version 3.5), but these logs will be collected via (Web Service Based Agent Bridge) HTTPS tunnel with additional encryption to the SecureMi® CMC and viewed through the CMC GUI.

The TOE Environment implements HTTPS support, which includes encryption/decryption (of CMC HTTPS management traffic between the TOE and the remote web browser used and to secure management traffic (Web Service Based Agent Bridge) between distributed SecureMi® Endpoint to SecureMi® CMC.

The .NET Framework 4.0 cryptography module is used to provide extra encryption on top of HTTPS tunnel. It provides the cryptographic primitives necessary to perform cryptographic functions, including encryption/decryption (AES), hashing, message authentication and compression.

To execute the justification action during a policy violation, SecureMi® Endpoint Super Agent software uses Namedpipe Based API to inform SecureMi® Endpoint Agent software on the duty to request justification text from the end-user. As soon as the SecureMi® Endpoint Agent software receives the instruction, it will query the SecureMi® Endpoint Cache Database for extra information before prompt the justification screen to the end-user. The .NET Framework 4.0 cryptography module is used to provide encryption (AES) for Namedpipe Based API communication.

SecureMi® Endpoint policy manager communicates with SecureMi® Endpoint Service via Socket Based API to obtain the software installation and patch updates command to run specific instructions during installation event. SecureMi® Endpoint Bridge Service also interacts with SecureMi® Endpoint Service on the same Socket Based API to manage on the installation and patch updates event. The .NET Framework 4.0 cryptography module is used to provide encryption (AES) for Socket Based API communication.

Exclusion from the TOE Boundary

The components excluded from the SecureMi® TOE boundary are given below. The justification for excluding these components is provided in the sections to follow.

- **SecureMi® CMC Database**

  SecureMi® CMC Database stores information about SecureMi® CMC authorized officers' credentials, the DLP policies, events and incidents in a database.

  SecureMi® CMC enforces access control and maintains integrity of these resources by performing only well-formed operations on these resources and only on behalf of authorized officers.

- **SecureMi® Endpoint Cache Database**

Some audit, event and incident logs captured by SecureMi® Endpoint are stored temporary in the client side database namely Endpoint Cache Database (SQL CE version 3.5), but will be downloaded via HTTPS tunnel with additional encryption to the SecureMi® CMC and viewed through the CMC GUI.

Justification of Exclusion

- **SecureMi® CMC Database**

  The justification for excluding the database from the SecureMi® TOE boundary is based on the following factors:

  Database security provided by SecureMi® CMC: This Security Target makes no claims about inherent database security. All access control to the database security is provided by SecureMi® CMC, not the database.

  Database functionality not mapped to SFRs: This Security Target makes no claims about database functionality (aside from the inherent, fundamental, and basic function of data storage). The Database operates only as a data warehouse for user and system data. Database functionality is not mapped to any of the SFRs in this Security Target.

  Well-defined database interface: The only interface to the database is through SecureMi® CMC and it uses the ODBC-API. That is, database access is only available through a well-defined interface (ODBC-API).

- **SecureMi® Endpoint Cache Database**

  The justification for excluding the database from the SecureMi® TOE boundary is based on the following factors:

  Database security provided by SecureMi® Endpoint: This Security Target makes no claims about inherent database security. All access control to the database security is provided by SecureMi® Endpoint, not the database.

  Database functionality not mapped to SFRs: This Security Target makes no claims about database functionality (aside from the inherent, fundamental, and basic function of data storage). The Database operates only as a data warehouse for user and system data. Database functionality is not mapped to any of the SFRs in this Security Target.

  Well-defined database interface: The only interface to the database is through SecureMi® Endpoint and it uses the ODBC-API. That is, database access is only available through a well-defined interface (ODBC-API).

Hardware, operating system platform and Microsoft Certificate Authority

The TOE makes no claims about the Windows operating system and software services and any hardware used.

The justification for excluding the abstract machine from the SecureMi® TOE boundary is based on the following factors:

Operating system: The TSF is enforced by the TOE and the SFRs are completely satisfied by TOE functions (aside from those with environmental dependencies). The operating system with which the TOE interfaces, is assumed to be trusted, meaning that it can be relied upon to correctly execute the TOE functions.

Hardware independence: The TOE software is optimized to execute any x86 (i.e., Intel or equivalent processor)-based machines, regardless of the hardware vendor. That is, any hardware platform that meets the minimum system requirements suffices.

2.3.2 Logical scope of the TOE

The following table (Table 3 – Logical security functions) describes the logical security functions provided by the TOE.

Table 3 – Logical security functions

TSF	Description
Security Audit	The Security Audit function provides the TOE with the functionality for generation and viewing of audit data. Authorized officers can view audit log entries captured by TOE through SECUREMI® CMC as the audit logs captured by SecureMi® Endpoint and SecureMi® Storage are forwarded to the SECUREMI® CMC where they can be viewed through the CMC GUI.
Identification and Authentication	Authorized officers must be identified and authenticated before they can perform any management tasks on the TOE or TOE data. Authorized officers authenticate to the SECUREMI® CMC with a user ID and password through a web browser. Once authorized officers are authenticated, they may perform management tasks as allowed by their permissions.
Security Management	Security Management functions define roles and role management functionality of the TOE. By default, the TOE comes with a few authorised officer roles such as Policy Manager, Incident Manager, Administrator and Super Administrator. The Super Administrator role can define one or more Limited authorized officer roles (such as default roles, Policy Manager, Incident Manager and Administrator), and assign permissions to them as appropriate. Each authorized officer is also assigned a user group and user ID, which help to further define the permissions granted. Alternative default values may be specified by the Super Administrator.
User Data Protection	The TOE allows authorized officers to enforce a rigid Administrative Access Control Rules and Policies for authorized officers accessing the TOE. The TOE enforces authorized officer-configurable policies on access to sensitive data: SecureMi® Endpoint requires the end-users to key-in correct OTP to retrieve on quarantined data on targeted machines. Data Discovery Policies enforce rules governing the suitability of files on targeted machines to store sensitive data. SecureMi® Endpoint provides secure vault for end-users to store sensitive data

3 CONFORMANCE CLAIMS (ASE_CCL)

3.1 COMMON CRITERIA CONFORMANCE CLAIMS

The ST and TOE are conformant to version 3.1 (Revision 4) of the Common Criteria for Information Technology Security Evaluation.

- **Part 2 conformant**. Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1, Revision 4.
- **Part 3 conformant**. Conformant with Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, Revision 4. The claimed assurance package is EAL2.

3.2 PROTECTION PROFILE CONFORMANCE CLAIMS

Neither the ST nor TOE claim conformance to any Protection Profiles.

4 SECURITY PROBLEM DEFINITION (ASE_SPD)

This section provides the description of the threats, organizational security policies that should be implemented in the TOE operational environment and assumptions defined as follows:

- Threats, which exist against the assets of the TOE and have to be countered by the TOE;
- Organizational security policies are the set of security rules and procedures that the TOE users and operational environment should comply with; and
- Assumptions are the aspects of the operational environment that are expected to be available in order for the TOE to perform securely.

4.1 THREATS

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

- Attackers who are not TOE authorized officers: 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 authorized officers: 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 authorized officers are, however, assumed not to be wilfully hostile to the TOE, and are therefore not included as threat agents in Table 2 below.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 5 Security Objectives. The following threats are applicable:

Table 4 - Threats

Threats	Description
T.MASQUERADE	A threat agent (attacker/s) may try to impersonate authorized personnel by stealing access credentials or any other methods.
T.UNAUTHACCESS	A threat agent (attacker/s) may try to gain unauthorized access to **SECUREMI® CMC** (access control) and other protected resources.
T.DISCLOSURE	A threat agent (attacker/s) may perform information network packet analysis attack by sniffing the data/information transacted between source and destinations of authorized IT entities without the knowledge of both users of these IT entities.
T.TSF_DATA_ALTERATION	A threat agent (attacker/s) may try to access the TOE or attack the system in order to change or delete the TOE configuration or get access to the functionality or TSF data.

T.RECORDFAILURE	A threat agent (attacker/s) may cause an action to tamper with TOE configuration or TOE storage so that TOE fails to record security related event properly.
T.MGMTFAILURE	The TOE may fail to response or mitigate the attacks performed by threat agent's (attacker/s) inappropriate action (e.g. leak by copying out of non-public or confidential information from the organization) taken on the TSF data that needs protection.
T.TAMPEREVIDENCE	A threat agent (attacker/s) may attempt to move, modify, or delete the incident logs and evidences.
T.UNAUTHACTION	A threat agent (attacker/s) may access the user data that needs to be protected according to **DLP** policy and take authorized action on it.

4.2 ORGANIZATION SECURITY POLICIES (OSP)

This section describes the complete set of organisational security policy statements or rules with which the TOE and/or its environment must comply.

Table 5 - Organizational security policies

OSP	Description
P.AUDIT	The TOE shall generate and maintain a record of security-related events to ensure accountability. Records shall be reviewed based on the timeline defined by the organizational audit process and procedures.
P.SECUREMGMT	Knowledgeable and competent TOE authorized officer/s shall be assigned to manage the TOE securely and keep the TSF data up to date.
P.STATISTICS	TOE authorized officer/s shall record, analyze and produce statistics on the data of audit and incident. TOE shall have reporting capabilities built-in inside or integrate with other authorized software/system to generated eligible reports.
P.INTERTRUSTEDCHANNEL	The TOE environment shall support inter-trusted channel (secure platform) to established secure communication among trusted IT entities.
P.POLICIES	The organization has in place policies and procedures to prevent unauthorized access to the TOE and its underlying environment.

4.3 ASSUMPTIONS

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

Table 6 - Assumptions

Assumptions	Description
A.PLATFORM	It is assumed that all hardware and third party software supporting the TOE are reliable and operating in good condition. All supporting third party software must be updated with services packs, fixes, patches and anti-virus patterns.
A.PHYSICAL	The TOE shall be located in physically secure environment that can be accessed only by the authorized personnel.
A.MAINTENANCE	When the internal network environment changes due to change in the network configuration, host and services service increase or decrease, the changed environment and security policy shall immediately be reflected in the TOE operation policy so that security level can be maintained to be as the same as before.
A.ADMIN	Authorized officers and users are non-hostile, appropriately trained, and follow all user guidance, installation guidance and configuration guidance.
A.SECURECOMM	It is assumed that the IT environment will provide a secure line of communication between distributed portions of the TOE and between the TOE and remote authorized officers.

5 OBJECTIVES (ASE_OBJ)

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 4). 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.

5.1 OBJECTIVES FOR THE TOE

The following is the list of Security Objectives of the TOE.

Table 7 - Security objectives for the TOE

Objective	Description
O.AUDIT	The TOE shall generate and maintain a record of security-related events to ensure accountability of the audit logs in tracing the source of events. It shall also provide a means to review the records.
O.DATAPROTECTION	The TOE shall be able to protect data and preventing data from being copy, paste, modify, alter and etc. into external media.
O.IDENTAUTH	The TOE shall be able to identify and authenticate the TOE user/s before granting an access to the TOE.
O.SELFTEMPERING	TOE shall protect itself from any form of unauthorized access or tampering to its functionality, thus including the data in order to maintain the integrity of the system data and audit records.
O.SECUREACCESS	The TOE shall be able to authenticate and allows only TOE authorized officer/s in accessing the security functionality and configuration and data.
O.AUDITREVIEW	The TOE shall provide TOE authorized officer/s with TOE functions to filter, review and sorting the audit records.
O.LEAKAGEMGMT	The TOE shall enforce the policy and shall performed relevant actions on the files/data that hold confidential or sensitive information, performed relevant actions during data/files transfer/transact, performed relevant actions during user's editing processes and access to the information.
O.STATISTIC	The TOE shall be able to provide real time monitoring of security relevant incidents based on configured security policy.

5.2 OBJECTIVES FOR THE ENVIRONMENT

The TOE Security Objective for Operating Environment as follows:

Table 8 - Security objectives for the environment

Assumptions	Description
OE.OSREINFORCEMNT	All hardware and third party software supporting the TOE are reliable and operating in good condition. All supporting third party software must be updated with services packs, fixes, patches and anti-virus patterns.
OE.PHYSICALSEC	The TOE shall be placed in secure environment that can only be accessed by authorized person only.
OE.TIMESTAMP	The IT environment shall provide the TOE with reliable timestamp for the TOE's use.
OE.TRUSTEDADMIN	The personnel responsible for the administration or monitoring of the TOE and workstation shall be trustworthy and competent. They shall receive the necessary training and elements to carry out their duties correctly.
OE.SECURECOMM	The IT Environment will provide the cryptographic functionality and protocols required for the TOE to securely transfer information between distributed portions of the TOE.
OE.MANAGEMENT	The organisation managing the TOE shall assign a TOE authorized officer/s with an efficient knowledge and competency in the means of managing the TOE and keep the TSF data up to date with the IT security implementations.
OE.SECURE_OS	There will be policies and procedures in place to ensure that access to the TOE and its underlying environment is appropriately controlled.

5.3 SECURITY OBJECTIVES RATIONALE

The following shows that the complete security problem definition (SPD) with all threats, OSPs and assumptions is covered in the objectives.

Table 9 - Security objectives rationale

SPD	Rationale
Security Objectives Rationale Related to Threats	
T.MASQUERADE A threat agent (attacker/s) may try to impersonate authorized personnel by stealing access credentials or any other methods.	With O.IDENTAUTH the TOE ensures that it identifies and authenticates the authorized officers. This analysis is valid when the TOE is not bypassed or tampered with. The environment must provide a safe environment for the TOE (OE.PHYSICALSEC) and trusted authorized officers (OE.TRUSTEDADMIN) to facilitate the TOE's self defence. OE.SECURECOMM requires that information being transmitted between the TOE and TOE authorized officers never be modified or disclosed. This prevents threat agents from capturing identification and authentication data as it is transmitted.
T.UNAUTHACCESS A threat agent (attacker/s) may try to gain unauthorized access to SECUREMI® CMC (access control) and other protected resources.	O.SECUREACCESS requires that the TOE allow only TOE authorized officers to manage its functions and data. This prevents unauthorized users from gaining access to security data on the TOE. This analysis is valid when the TOE is not bypassed or tampered with. The environment must provide a safe environment for the TOE (OE.PHYSICALSEC) and trusted authorized officers (OE.TRUSTEDADMIN) to facilitate the TOE's self defence.
T.DISCLOSURE A threat agent (attacker/s) may perform information network packet analysis attack by sniffing the data/information transacted between source and destinations of authorized IT entities without the knowledge of both users of these IT entities	OE.SECURECOMM requires that information being transmitted between the TOE and TOE authorized officers never be modified or disclosed. This prevents threat agents from capturing identification and authentication data as it is transmitted.

SPD	Rationale
T.TSF_DATA_ALTERATION A threat agent (attacker/s) may try to access the TOE or attack the system in order to change or delete the TOE configuration or get access to the functionality or TSF data.	O.IDENTAUTH requires that the TOE identify and authenticate authorized officers before allowing any TSF-mediated activity to be performed by them. This prevents unauthorized users from accessing the TOE to change or delete the TOE configuration or get access to the functionality or TSF data. O.SECUREACCESS requires that the TOE ensure that only authorized officers be granted access to the data of the TOE. This prevents unauthorized users from accessing the TOE to change or delete the TOE configuration or get access to the functionality or TSF data. OE.SECURECOMM requires that the information passing between separate parts of the TOE and between the TOE and trusted remote authorized officers be protected from unauthorized disclosure and modification. This prevents unauthorized users from accessing the TOE to change or delete the TOE configuration or get access to the functionality or TSF data.
T.RECORDFAILURE A threat agent (attacker/s) may cause an action to tamper with TOE configuration or TOE storage so that TOE fails to record security related event properly.	O.SELFTEMPERING requires that TOE stores an encrypted copy of quarantined file in its endpoint's system to prevent it from tempering. O.SELFTEMPERING requires that TOE encrypts its fingerprint files at the endpoint as well as in the server to prevent attacker/s tempering.

SPD	Rationale
T.MGMTFAILURE The TOE may fail to responnd or mitigate the attacks performed by threat agent's (attacker/s) inappropriate action taken on the TSF data that needs protection.	OE.MANAGEMENT requires that TOE authorized officer/s to keep TOE and TSF data up to date to avoid fail to response or mitigate the attacks performed by threat agent's (attacker/s) inappropriate action taken on the TSF data that needs protection. For example, authorized officer/s fail to update TOE security policy to protect a document marks as non-public or confidential information due to lack of knowledge. OE.MANAGEMENT and O.STATISTIC requires that TOE authorized officer/s to monitor and response to the TOE security relevant incidents. For example, authorized officer/s should query the users who trigger an incident.
T.TAMPEREVIDENCE A threat agent (attacker/s) may attempt to move, modify, or delete the incident logs and evidences.	O.SELFTEMPERING requires that TOE stores an encrypted copy of evidence file in its endpoint's system to prevent it from tempering. O.IDENTAUTH requires that authorized officers of the TOE be identified and authenticated before allowing any TSF-mediated activity to be performed by them. This prevents unauthorized users from move, modify, or delete the incident logs and evidences. O.SECUREACCESS requires that the TOE ensure that only authorized officers be granted access to the TOE data. This prevents unauthorized users from move, modify, or delete the incident logs and evidences. OE.SECURECOMM requires that information passing between separate parts of the TOE and between the TOE and trusted remote authorized officers be protected from unauthorized disclosure and modification. This prevents unauthorized users from move, modify, or delete the incident logs and evidences.

SPD	Rationale
T.UNAUTHACTION A threat agent (attacker/s) may access the user data that needs to be protected according to DLP policy and take authorized action on it.	O.LEAKAGEMGMT requires that the TOE take specified actions on transmissions, end-user actions, and files identified as containing or accessing non-public or confidential information. This prevents threat agents from accessing that information. O.DATAPROTECTION requires that the TOE protect sensitive data and preventing sensitive data from being copy, paste, modify, alter and etc. into external media.
Security Objectives Rationale Related to OSPs	
P.AUDIT The TOE shall generate and maintain a record of security-related events to ensure accountability. Records shall review based on the timeline defined by the organizational audit process and procedures.	O.AUDIT requires that generate and maintain a record of security-related events to ensure accountability. Records shall review based on the timeline defined by the organizational audit process and procedures. O.AUDITREVIEW. The TOE has the capabilities to provide TOE authorized officer/s with TOE functions to filter, review and sorting the audit records including filter the audit record based on a timeline defined him/her. OE.TIMESTAMP. The TOE environment provides reliable timestamp for TOE's audit records.
P.SECUREMGMT Knowledgeable and competent TOE authorized officer/s shall be assigned to manage the TOE securely and keep the TSF data up to date.	OE.MANAGEMENT requires that TOE authorized officer/s manage the TOE securely and keep the TSF data up to date.
P.STATISTICS TOE authorized officer/s shall record, analyze and produce statistics on the data of audit and incident. TOE shall have reporting capabilities built-in inside or integrate with other authorized software/system to generated eligible reports.	O.STATISTICS requires that the TOE provide statistical report on the data of audit and incident.
P.INTERTRUSTEDCHANNEL The TOE environment shall support inter-trusted channel (secure platform) to established secure communication among the trusted IT entities.	OE.SECURECOMM ensures that the TOE environment provides the necessary means for protecting sensitive data transmitted between distributed TOE subsystems and end users.

SPD	Rationale
P.POLICIES The organization has in place policies and procedures to prevent unauthorized access to the TOE and its underlying environment.	OE.SECURE_OS ensure there are organizational policies and procedures in place to ensure that access to the TOE and its underlying environment is appropriately controlled.
Security Objectives Rationale Related to Assumptions	
A.PLATFORM It is assumed that all hardware and third party software supporting the TOE are reliable and operating in good condition. All supporting third party software must be updated with services packs, fixes, patches and anti-virus patterns.	OE.OSREINFORCEMNT ensures that all hardware and third party software supporting the TOE are reliable and operating in good condition. All supporting third party software must be updated with services packs, fixes, patches and anti-virus patterns.
A.PHYSICAL The TOE shall be located in physically secure environment that can be accessed only by the authorized personnel.	OE.PHYSICALSEC ensures that the TOE shall reside in a physically secure location, thereby preventing unauthorized physical access.
A.MAINTENANCE When the internal network environment changes due to change in the network configuration, host and services service increase or decrease, the changed environment and security policy shall immediately be reflected in the TOE operation policy so that security level can be maintained to be as the same as before.	OE.OSREINFORCEMNT ensures that all hardware and third party software supporting the TOE are reliable and operating in good condition. All supporting third party software must be updated with services packs, fixes, patches and anti-virus patterns. OE.MANAGEMENT requires that TOE authorized officer/s to keep TOE security policy so that security level can be maintained to be as the same as before.
A.ADMIN Authorized officers and users are non-hostile, appropriately trained, and follow all user guidance, installation guidance and configuration guidance.	OE.TRUSTEDADMIN ensures that TOE authorized officers are non-hostile, appropriately trained, and follow all guidance.
A.SECURECOMM It is assumed that the IT environment will provide a secure line of communication between distributed portions of the TOE and between the TOE and remote authorized officers.	OE.SECURECOMM ensures that the TOE Environment provides the necessary means for protecting sensitive data transmitted between distributed TOE subsystems and end users.

6 EXTENDED COMPONENTS DEFINITION (ASE_ECD)

Not applicable: no extended components have been defined.

7 SECURITY REQUIREMENTS (ASE_REQ)

7.1 SECURITY FUNCTIONAL REQUIREMENTS LIST

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 (Rev 4) of the CC, Part 2 providing functional requirements and Part 3 providing assurance requirements.

The following table (Table 10 – Security Functional Requirements (SFRs)) lists the Security Functional Requirements (SFR) defined and enforced by the TOE.

Table 10 – Security Functional Requirements (SFRs)

SFR	SFR Name	SFR Dependencies
FAU: Security Audit		
FAU_GEN.1	Audit data generation	FPT_STM.1 Reliable time stamps
FAU_SAR.1	Audit review	FAU_GEN.1 Audit data generation
FDP: User Data Protection		
FDP_ACC.1	Subset access control	FDP_ACF.1 Security attribute based access control
FDP_ACF.1	Security attribute based access control	FDP_ACC.1 Subset access control
		FMT_MSA.3 Static attribute initialization
FDP_IFC.1	Subset information flow control	FDP_IFF.1 Simple security attribute
FDP_IFF.1	Simple security attributes	FDP_IFC.1 Subset information flow control
		FMT_MSA.3 Static attribute initialization
FIA: Identification and Authentication		
FIA_SOS.2	TSF Generation of secrets	N/A
FIA_UAU.2	User authentication before any action	FIA_UID.1 Timing of identification
FIA_UAU.7	Protected authentication feedback	FIA_UAU.1 Timing of authentication
FIA_UID.2	User identification before any action	N/A
FMT: Security Management		
FMT_MOF.1	Management of security	FMT_SMR.1 Security roles

SFR	SFR Name	SFR Dependencies
	functions behavior	FMT_SMF.1 Specification of management functions
FMT_MSA.1	Management of security attributes	FDP_ACC.1 Subset access control; **or** FDP_IFC.1 Subset information flow control
		FMT_SMR.1 Security roles
		FMT_SMF.1 Specification of management functions
FMT_MSA.3	Static attribute initialization	FMT_MSA.1 Management of security attributes
		FMT_SMR.1 Security roles
FMT_MTD.1	Management of TSF data	FMT_SMR.1 Security roles
		FMT_SMF.1 Specification of management functions
FMT_SMF.1	Specification of management functions	N/A
FMT_SMR.1	Security roles	FIA_UID.1 Timing of identification

7.2 SECURITY AUDIT (FAU)

7.2.1 Audit data generation (FAU_GEN.1)

Hierarchical to No other components

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

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

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

c. [The following management functions:

- Create, modify, delete authorized officers;
- Create, modify, delete groups;
- Create, modify, delete credentials;
- Assignment of endpoint agent group;
- Assignment of storage agent group;
- Successful login;
- Logout;
- Failed login; and
- Create, modify, delete, synchronize DLP policies.

]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

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

b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [no other audit relevant information]

Dependencies FPT_STM.1 Reliable time stamps

Application note Start-up and shutdown of the audit functions are implied by the initiation and cessation of the generation of any audit records.

7.2.2 Audit review (FAU_SAR.1)

Hierarchical to No other components

FAU_SAR.1.1 The TSF shall provide **[**SECUREMI® CMC's authorized officers] with the capability to read **[**all audit information stored by the SECUREMI® CMC in the CMC database through CMC GUI] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the ~~user~~ authorized officer to interpret the information.

Dependencies FAU_GEN.1 Audit data generation

7.3 USER DATA PROTECTION (FDP)

7.3.1 Subset access control (FDP_ACC.1)

Hierarchical to No other components.

FDP_ACC.1.1 The TSF shall enforce the **[**SECUREMI® CMC access control SFP**]** on [

- Subjects**:** users (authorized officers or end users) attempting to establish an interactive session with the TOE.
- Objects**:** User interface menu items, policies, incidents, events, reports, administrative management data, and credentials.
- Operations**:** All interactions between the subjects and objects identified above.

]

Dependencies FDP_ACF.1 Security attribute based access control

7.3.2 Security attribute based access control (FDP_ACF.1)

Hierarchical to No other components.

FDP_ACF.1.1 The TSF shall enforce the [SECUREMI® CMC access control SFP] to objects based on the following: [

- Subject attributes:
- Officer ID
- Officer Role
- Officer Group
- Officer's permission
- Object attributes:
- Permissions assigned to objects
- Absence of permission assigned to objects

]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- If the subject has the authorized officer role, access is granted.
- If a subject requests access to an object that has no assigned permissions, access is granted.
- If a subject who does not have the authorized officer role request access to an object that has assigned permissions, the permissions of the subject are examined to determine if the subject has permission to access the object. If a match is found, access is granted.
- If none of the above rules apply, access is denied.

]

FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [no additional rules].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on [no additional rules].
Dependencies	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

7.3.3 Subset information flow control (FDP_IFC.1)

Hierarchical to No other components.

FDP_IFC.1.1 The TSF shall enforce the [SecureMi® Endpoint information flow control SFP] on [

- Subjects: Endpoint machine user attempting to transfer or transmit non-public or confidential or sensitive data
- Information: Files and content stored on the endpoint machine transferred from the endpoint machine
- Operations:
- Log down incident event;
- Block and quarantine file(s);
- Request justification; or
- Send email notification to authorized officer.

]

Dependencies FDP_IFF.1 Simple security attributes

7.3.4 Simple security attributes (FDP_IFF.1)

Hierarchical to No other components.

FDP_IFF.1.1 The TSF shall enforce the [SecureMi® Endpoint information flow control SFP] based on the following types of subject and information security attributes: [

- **Subject attributes:**
  - Agent ID; and
  - Agent Group
- **Information attributes:**
  - Keyword or phrase list
  - Expression or character patterns
  - Fingerprints of specific sensitive documents
  - File attributes
  - Protocol
  - MAC Address
  - Memory content
  - DLP device detected

]

FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[** • Evaluate the configured policy rules and • Record an event if the result of the evaluation is “Log”. • Notify an event to the related authorized officer’s group if the result of the evaluation is “Notify”. • Request for justification text from end user to justify an event if the result of the evaluation is “Justify”. • Make a copy and keep the data as evidence if the result of the evaluation is “Keep Evidence”. • Block the transmission or quarantine the data if the result of the evaluation is “Block”. • Encrypt the data if the result of the evaluation is “Encrypt”.]
FDP_IFF.1.3	The TSF shall enforce the [no additional information flow control SFP rules].
FDP_IFF.1.4	The TSF shall explicitly authorize an information flow based on the following rules: [no additional rules].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [no additional rules].
Dependencies	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation

7.4 IDENTIFICATION AND AUTHENTICATION (FIA)

7.4.1 TSF Generation of secrets (FIA_SOS.2)

Hierarchical to No other components

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet [no standard].

FIA_SOS.2.1 The TSF shall be able to enforce the use of TSF generated secrets for [retrieving files from quarantine, temporarily suspending DLP protection].

Dependencies No dependencies

7.4.2 User authentication before any action (FIA_UAU.2)

Hierarchical to FIA_UAU.1 Timing of authentication

FIA_UAU.2.1 The TSF shall require each ~~user~~ authorized officer to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that ~~user~~ authorized officer.

Dependencies FIA_UID.1 Timing of identification

7.4.3 Protected authentication feedback (FIA_UAU.7)

Hierarchical to No other components.

FIA_UAU.7.1 The TSF shall provide only [obscured] feedback to the ~~user~~ authorized officer while the authentication is in progress.

Dependencies FIA_UAU.1 Timing of identification

7.4.4 User identification before any action (FIA_UID.2)

Hierarchical to FIA_UID.1 Timing of identification

FIA_UID.2.1 The TSF shall require each ~~user~~ authorized officer to be successfully identified before allowing any other TSF-mediated actions on behalf of that ~~user~~ authorized officer.

Dependencies No dependencies.

7.5 SECURITY MANAGEMENT (FMT)

7.5.1 Management of security functions behaviour (FMT_MOF.1)

Hierarchical to No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behaviour of, modify the behaviour of*] the functions **[**

- Management of users, groups, credentials and roles;
- Management of SecureMi® Endpoint Configuration;
- Management of SecureMi® Storage Configuration;
- Management of DLP Policies;
- Management of DLP Setting (Including Pattern);
- Management of Reports;
- System Configuration;
- Management of Notification Templates or Alert Dialogs;
- Retrieval of Unlock OTP for End User to access quarantined files; and
- Policy Synchronization to Agent Groups.

] to [

- Super Administrators; and
- Limited authorized officers (when given permission by the authorized officer role)

].

Dependencies FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Application note This SFR defines the general requirements for the DLP system

7.5.2 Management of security attributes (FMT_MSA.1)

Hierarchical to No other components.

FMT_MSA.1.1 The TSF shall enforce the [SECUREMI® CMC Authorization] to restrict the ability to *[change_default, query, modify, delete]* the security attributes **[**

- Authorized Officer role;
- Authorized Officer;
- Authorized Officer group;
- Authorized Officer permissions;
- Permissions assigned to objects;
- Credentials

] to [

- the Super Administrator; and/or
- Limited Authorized Officer Roles

].

Dependencies [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

7.5.3 Static attribute initialization (FMT_MSA.3)

Hierarchical to No other components.

FMT_MSA.3.1 The TSF shall enforce the [SFPs listed in Table 11 - Static attribute SFPs] to provide [*restrictive*] default values for security attributes that are used enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **[**Super Administrator and limited authorized officer role(s)**]** 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

Table 11 - Static attribute SFPs

Security Attributes	**SECUREMI® CMC Access Control SFP**	**SecureMi® Endpoint SFP**	**SecureMi® Storage SFP**
Officer Role	Restrictive	n/a	n/a
Officer	Restrictive	n/a	n/a
Officer Group	Restrictive	n/a	n/a
Officer Permissions	Restrictive	n/a	n/a
Object Permissions	Restrictive	n/a	n/a
Credentials	Restrictive	n/a	n/a
Agent	Restrictive	n/a	n/a
Agent Group	Restrictive	n/a	n/a
Keyword/Phrases List	Restrictive	n/a	n/a
Expression/Character pattern	Restrictive	n/a	n/a
Document Fingerprint	Restrictive	n/a	n/a
File Type	Restrictive	n/a	n/a
Protocol	Restrictive	n/a	n/a
DLP Device	Restrictive	n/a	n/a

7.5.4 Management of TSF data (FMT_MTD.1)

Hierarchical to No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to [*change_default, query, modify, delete*] the [DLP settings and policies] to [the Super Administrator, Limited authorized officer Roles].

Dependencies FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Application note Major features that effect the operation of DLP systems such as create, modify, delete policies, change default, query and delete by the authorized officer or a person given the rights.

7.5.5 Specification of Management Functions (FMT_SMF.1)

Hierarchical to No other components.

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

- Authorized officer account management;
- DLP policy enforcement management;
- Incident log management;
- One-Time Password (OTP) generation; and
- Audit log management

]

Dependencies No dependencies.

7.5.6 Security roles (FMT_SMR.1)

Hierarchical to No other components.

FMT_SMR.1.1 The TSF shall maintain the roles: [

- Policy Manager (authorized officer with authorization to enforce DLP policy);
- Incident Manager (authorized officer with authorization to manage incidents);
- Administrator (authorized officer with authorization to manage the TOE); and
- Super Administrator (authorized officer with authorization to access all management functions)

].

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

Dependencies FIA_UID.1 Timing of identification

7.6 SECURITY ASSURANCE REQUIREMENTS

Assurance class	Assurance component
ADV Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
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
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
ATE Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

8 SECURITY REQUIREMENTS RATIONALE

All open operations have been performed as indicated in the chapter "**Error! Reference source not found.**".

8.1 SAR RATIONALE

This ST contains the assurance requirement from the CC EAL2 assurance package and was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. This ST has been developed for a generalized environment.

8.1.1 SAR dependencies rationale

The SARs of the ST are defined as EAL2. All EALs are consistent and all dependencies are met.

8.2 SFR RATIONALE

The following table provides a mapping between the security objectives defined in Section 5.1 (Objectives for the TOE) and the SFRs defined in Section 7 (Security Requirements (ASE_REQ)).

Table 9 – SFR to Objective rationale

Security objective for the TOE	SFR(s)	Rationale
O.AUDIT The TOE shall generate and maintain a record of security-related events to ensure accountability of the audit logs in tracing the source of events. It shall also provide a means to review the records.	FAU_GEN.1 Audit data generation	The SFR meets the objective by generating logs for management actions on the TOE.
	FMT_SMF.1 Specification of Management Functions	The SFR meets the objective by allowing authorized officers to access audit logs.
O.DATAPROTECTION The TOE shall be able to protect data and preventing data from being copy, paste, modify, alter and etc. into external media.	FDP_IFC.1 Subset information flow control	The SFR meets the objective by ensuring that end-users are restricted in copy and paste, modify and alter data containing sensitive information into external media such as USB flash drive, according to the DLP Policy.
O.IDENTAUTH The TOE shall be able to identify and authenticate the TOE user/s before granting an	FIA_SOS.2 TSF Generation of secrets	The SFR meets the objective by allowing the generation of One-Time Passwords.

Security objective for the TOE	SFR(s)	Rationale
access to the TOE.	FIA_UAU.2 User authentication before any action	The SFR meets the objective by requiring that TOE authorized officers be successfully authenticated before allowing any TSF-mediated actions to be performed by them.
	FIA_UID.2 User identification before any action	The SFR meets the objective by requiring that TOE authorized officers be successfully identified before allowing any TSF-mediated actions to be performed by them.
	FMT_SMR.1 Security roles	The SFR meets the objective by associating users with TOE-defined roles.
O.SELFTEMPERING TOE shall protect itself from any form of unauthorized access or tampering to its functionality, thus including the data in order to maintain the integrity of the system data and audit records.	FMT_MTD.1 Management of TSF data	The SFR meets the objective by ensuring that only authorized officers have the ability to change default, query, modify and delete the DLP policy that effect the operation of DLP systems.
O.SECUREACCESS The TOE shall be able to sanitize and allows only TOE authorized officer/s in accessing the security functionality and configuration and data.	FMT_MSA.1 Management of security attributes	The SFR meets the objective by requiring that only the authorized officer roles be permitted to perform all management actions on the TOE.
	FMT_MSA.3 Static attribute initialization	The TSF meets the objective by enforcing the SECUREMI® CMC to provide default values for security attributes that are used enforce the SFP.

Security objective for the TOE	SFR(s)	Rationale
	FMT_MOF.1 Management of security functions behaviour	The SFR meets the objective by ensuring that appropriate functions are provided for managing the TOE and TSF data.
	FMT_MTD.1 Management of TSF data	The SFR meets the objective by ensuring that only authorized officers have the ability to change default, query, modify, delete and clear the DLP policy that effect the operation of DLP systems.
	FIA_UAU.7 Protected authentication feedback	The SFR meets the objective by ensuring that the TOE provides only obscured feedback to authorized officers during authentication.
	FMT_SMR.1 Security roles	The SFR meets the objective by associating users with TOE-defined roles.
O.AUDITREVIEW The TOE shall provide TOE authorized officer/s with TOE functions to filter, review and sorting the audit records.	FAU_SAR.1 Audit review	The SFR meets the objective by allowing review of audit logs generated by the TOE.
	FMT_SMF.1 Specification of Management Functions	The SFR meets the objective by allowing authorized officers to access audit logs.
O.LEAKAGEMGMT The TOE shall enforce the policy and shall performed relevant actions on the files/data that hold confidential or sensitive information, performed relevant actions during data/files transfer/transact, performed relevant actions during user's editing processes and access to the information.	FDP_ACC.1 Subset access control	The SFR meets the objective by ensuring that end-users are restricted in transmitting data containing sensitive information, according to the DLP Policy.
	FDP_ACF.1 Security attribute based access control	The SFR meets the objective by enforcing the DLP Policy, by which end users are restricted from transmitting data containing sensitive information.

Security objective for the TOE	**SFR(s)**	**Rationale**
	FDP_IFC.1 Subset information flow control	The SFR meets the objective by ensuring that end-users are restricted in transmitting data containing sensitive information, according to the DLP Policy.
	FDP_IFF.1 Simple security attributes	The SFR meets the objective by enforcing the DLP Policy, by which end-users are restricted from transmitting data containing sensitive information.
O.STATISTIC The TOE shall be able to provide real time monitoring of security relevant incidents based on configured security policy.	FAU_SAR.1 Audit Review	The SFR meets the objective by providing audit records in a form of graphical statistical chart suitable for the TOE authorized officer to interpret the information.
	FMT_MOF.1 Management of security functions behaviour	The SFR meets the objective by providing authorized officers with the functions to configure the reporting capability.

8.2.1 SFR dependencies rationale

The following table shows the SFR dependencies and whether they are met.

Table 10: SFR Dependencies Rationale

SFR	Dependencies	Met?
FAU_GEN.1	FPT_STM.1	Timestamps are provided by the operational environment, therefore this dependency is met.
FAU_SAR.1	FAU_GEN.1	Yes
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1	Yes
	FMT_MSA.3	Yes
FDP_IFC.1	FDP_IFF.1	Yes
FDP_IFF.1	FDP_IFC.1	Yes
	FMT_MSA.3	Yes
FIA_SOS.2	None	Yes
FIA_UAU.2	FIA_UID.1	Yes (by FIA_UID.2)
FIA_UAU.7	FIA_UAU.1	Yes (by FIA_UAU.2)
FIA_UID.2	None	Yes
FMT_MOF.1	FMT_SMR.1	Yes
	FMT_SMF.1	Yes
FMT_MSA.1	FDA_ACC.1	Yes
	FMT_SMR.1	Yes
	FMT_SMF.1	Yes
FMT_MSA.3	FMT_MSA.1	Yes
	FMT_SMR.1	Yes
FMT_MTD.1	FMT_SMR.1	Yes
	FMT_SMF.1	Yes
FMT_SMF.1	None	Yes
FMT_SMR.1	FIA_UID.1	Yes

9 TOE SUMMARY SPECIFICATION (ASE_TSS)

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.

9.1 SECURITY AUDIT

The Security Audit function provides the TOE with the functionality for generation and viewing of audit data. The TOE captures logs of management events such as policy changes and management of device credentials.

The SECUREMI® CMC and each of the SECUREMI® Endpoint generate audit logs. Each of the SECUREMI® Endpoints upload audit logs to the SECUREMI® CMC, which then stores them on the CMC database. Authorized officers can then analyse. Authorized officers can view audits captured by the TOE through the SECUREMI® CMC GUI. Sometimes TOE will notify the TOE authorized officer on the policy violation according to the setting of DLP Policy.

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

9.2 USER DATA PROTECTION

The TOE allows authorized officers to enforce a rigid Administrative Role Based Access Control Policy for authorized officers accessing the TOE. Authorized officers with the Super Administrator have permission to perform any and all administrative functions on the TOE. Other authorized officers may access user interface menu items, policies, incidents, events, reports, administrative management data, and device credentials if given the appropriate permissions by the Super Administrator. Access is granted to objects based on the authorized officer's user ID and group.

The TOE enforces authorized officer-configurable DLP Policies on access to sensitive data, as follows:

The SecureMi® Endpoint Super Agent uses 4 methods (pattern matching techniques) for detecting sensitive content:

- Creating keyword or phrases list that match sensitivity criteria of the content to be detected;
- Creating expression or character patterns that match sensitivity criteria of the content to be detected;
- Creating fingerprints of specific sensitive documents; and
- File attributes or characters such as file type and file size.

In addition to detection rules, each DLP policy also implements product-specific rules that detect attributes that may or may not be allowed such as:

- Protocol characteristics, such as SMTP,
- Device characteristics, such as a device's name, USB flash drive information or printer name; and/or
- Memory content

Policy actions are automatically performed by a DLP product when specified rules are matched. Possible policy actions include the following:

- Log;

- Notify;
- Justify;
- Keep Evidence; and/or
- Block

The action taken is dependent on the resource\channel in which the alert was raised. Table 12 – Resource identifies the policy implemented by the TOE.

Table 12 – Resource Channel \ Policy Action Relationships

Resource channel \ Action	Log Action	Notify Action	Justify Action	Keep Evidence Action	Block Action
Data Discovery	Incident event will be logged in the system for reporting if turn on.	Incident event will be emailed to the preferred authorized officer group if turn on.	Not applicable.	If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched.	If turn on, in the event of an incident, a block action quarantine file (provided that file was not controlled by other process, otherwise that file will be unable to be deleted) by removing the original file from its location and keep secretly within TOE system in encrypted form. However, user can request an Unlock Code from the authorized officer to recover the quarantine files.
Removable Storage Data	Incident event will be logged in the system for reporting if turn on.	Incident event will be emailed to the preferred authorized officer group if turn on.	If turn on, in the event of an incident, a justify action causes a popup message to appear to the end-user, requiring the end-user to provide text justifying the attempted	If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched.	If turn on, in the event of an incident, a block action quarantine file (provided that file was not controlled by other process, otherwise that file will be unable to be deleted) by removing the original file from its location and keep secretly within TOE system in encrypted form. However, user can request an Unlock Code from the authorized officer to recover the quarantine files. A block action also

			action.		eject the device (if it is not being controlled) eventually.
Removable Storage Device	Incident event will be logged in the system for reporting.	Incident event will be emailed to the preferred authorized officer group if turn on.	If turn on, in the event of an incident, a justify action causes a popup message to appear to the end-user, requiring the end-user to provide text justifying the attempted action.	Not applicable.	Eject the device (if it is not being controlled) if the device is not registered into the white list.
Email	Incident event will be logged in the system for reporting if turn on.	Incident event will be emailed to the preferred authorized officer group if turn on.	If turn on, in the event of an incident, a justify action causes a popup message to appear to the end-user, requiring the end-user to provide text justifying the attempted action.	Attach file: If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched. Key in message: Not applicable Clipboard file drop: If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched.	Attach file: If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched. Key in message: Not applicable Clipboard file drop: If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched.
Clipboard	Incident event will be logged in the system for reporting	Incident event will be emailed to the preferred authorized	If turn on, in the event of an incident, a justify action	Not applicable.	If turn on, in the event of an incident, a block action erase the clipboard content.

	if turn on.	officer group if turn on.	causes a popup message to appear to the end-user, requiring the end-user to provide text justifying the attempted action.		
Print Screen	Incident event will be logged in the system for reporting fi turn on.	Not applicable.	If turn on, in the event of an incident, a justify action causes a popup message to appear to the end-user, requiring the end-user to provide text justifying the attempted action.	Not applicable.	If turn on, in the event of an incident, a block action erase the clipboard content.
HTTP	Incident event will be logged in the system for reporting.	Incident event will be emailed to the preferred authorized officer group if turn on.	If turn on, in the event of an incident, a justify action causes a popup message to appear to the end-user, requiring the end-user to provide text justifying the	Attach file: If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched. Key in message: Not applicable Clipboard file drop: If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched.	Not applicable.

<table>
<tr><td></td><td></td><td></td><td>attempted action.</td><td></td><td></td></tr>
<tr><td>FTP</td><td>Incident event will be logged in the system for reporting if turn on.</td><td>Incident event will be emailed to the preferred authorized officer group if turn on.</td><td>If turn on, in the event of an incident, a justify action causes a popup message to appear to the end-user, requiring the end-user to provide text justifying the attempted action.</td><td>Attach file: If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched.
Key in message: Not applicable
Clipboard file drop: If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched.</td><td>Not applicable.</td></tr>
<tr><td>Peer-to-peer</td><td>Incident event will be logged in the system for reporting if turn on.</td><td>Incident event will be emailed to the preferred authorized officer group if turn on.</td><td>Not applicable.</td><td><table><tr><td>Attach file</td><td>If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched.</td></tr><tr><td>Key in message</td><td>Not applicable</td></tr><tr><td>Clipboard file drop</td><td>If turn on, in the event of an incident, a keep evidence action keeps file as evidence, the original file remains untouched.</td></tr></table></td><td>Not applicable.</td></tr>
<tr><td>Instant Messaging</td><td>Incident event will</td><td>Incident event will</td><td>Not applicable.</td><td></td><td>Not applicable.</td></tr>
</table>

	be logged in the system for reporting if turn on.	be emailed to the preferred authorized officer group if turn on.			
Printer	Incident event will be logged in the system for reporting if turn on.	Incident event will be emailed to the preferred authorized officer group if turn on.	If turn on, in the event of an incident, a justify action causes a popup message to appear to the end-user, requiring the end-user to provide text justifying the attempted action.	Not applicable.	If turn on, in the event of an incident, a block action delete the print job (if the length of time for the print job to print is long enough for the TOE to filter it).

The TOE supports Unknown and Invalid File Type except for data discovery policy type. File types that are unable to extract text file (e.g. *.exe file) is defined as unknown file type. If user change a PDF file (says, abc.pdf) to different extension (says, abc.zip), system will defined this as invalid file type. Both unknown and invalid file type will trigger an incident. The TOE also disables the file drag and drop function.

Each policy action taken is captured in an event record, and passed to the SECUREMI® CMC for viewing by the authorized officer.

In addition, SecureMi® Endpoint requires the end-users to key-in correct OTP to retrieve on quarantined data on targeted machines. Data Discovery Policies enforce rules governing the suitability of files on targeted machines to store sensitive data. SecureMi® Endpoint provides secure vault for end-users to store sensitive data

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1.

9.3 IDENTIFICATION AND AUTHENTICATION

Authorized officers must be identified and authenticated before they can perform any management tasks on the TOE or TOE data. Authorized officers authenticate to the SecureMi® CMC with a user ID and password through a web browser. Once authorized officers are authenticated, they may perform management tasks as allowed by their permissions.

The TOE provides authorized officers with obscured feedback only (*'s) while they are entering sensitive authentication data (i.e. passwords).

The TOE supports the generation of one-time passwords to allow Endpoint users to retrieve quarantined files or to temporarily suspend their DLP protection.

TOE Security Functional Requirements Satisfied: FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FIA_SOS.2

9.4 SECURITY MANAGEMENT

Security Management functions define roles and role management functionality of the TOE. The TOE maintains a Super Administrator role, which has access to all TOE management functionality.

The Super Administrator role can define one or more limited authorized officer roles (such as default roles, Policy Manager, Incident Manager and Administrator), and assign permissions to them as appropriate.

Each authorized officer is also assigned a user group and user identifier (ID), which help to further define the permissions granted.

The functions authorized officers may manage, depending on permissions granted, include: users, groups, roles, credentials, SecureMi® Storage configuration, SecureMi® Endpoint configuration, SecureMi® CMC Configuration, pattern matching methods and logics, notification email server configuration, message notification templates, policies, policy synchronization to DLP agent group, reports, product license, generate an unlock OTP for end user to retrieve quarantined data, generate a switch off OTP for end user to temporary by pass SecureMi® Endpoint functions, incidents, and events.

Restrictive default values for security attributes defined by the Access Control Policies are enforced by the TSF, and alternative default values may be specified by the Super Administrator.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.