EMC Corporation

EMC SourceOne™ File Systems v7.2, Email Management v7.2, Discovery Manager v7.2, and for Microsoft SharePoint v7.1

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.6

Prepared for:

EMC Corporation
176 South Street
Hopkinton, MA 01748
United States of America

Phone: +1 508 435 1000
http://www.emc.com

Prepared by:

Corsec Security, Inc.
13921 Park Center Road
Herndon, VA 20171
United States of America

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

Table of Contents

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table of Figures

List of Tables

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is the EMC SourceOne™ File Systems v7.2, Email Management v7.2, Discovery Manager v7.2, and for Microsoft SharePoint v7.1, and will hereafter be referred to as the TOE throughout this document. The TOE is a software-based, distributed solution that archives content from email, file, and Microsoft SharePoint servers and provides advanced role-based search and discovery capabilities.

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 functionality 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 (OSPs), 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 Security 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	EMC Corporation EMC SourceOne™ File Systems v7.2, Email Management v7.2, Discovery Manager v7.2, and for Microsoft SharePoint v7.1 Security Target
ST Version	Version 1.5
ST Author	Corsec Security, Inc.
ST Publication Date	2015-11-04
TOE Reference	SourceOne™ Email Management v7.2 build 7.20.2524 SourceOne™ Discovery Manager v7.2 build 7.20.2524 SourceOne™ for File Systems v7.2 build 7.20.2524 SourceOne™ for Microsoft SharePoint v7.1 build 7.12.2075

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.3 Product Overview

EMC SourceOne is an enterprise solution that archives, retains, and organizes email, file, and Microsoft SharePoint server content to reduce storage costs and satisfy compliance and legal discovery requirements. EMC SourceOne archives and organizes content from Microsoft Exchange, IBM[1] Lotus Domino, and SMTP[2] mail servers, as well as from Microsoft SharePoint and network file servers. Archived content is stored in a centrally managed archive. Search, restore, and export capabilities are available to authorized users through a search web interface, an archive search site integrated into SharePoint, and an application designed specifically for legal discovery searches. All archived content is tagged with a unique message identifier generated using an EMC proprietary hash of object data and properties. This ensures the integrity of the archived content. The unique message identifier is also used for deduplication to reduce storage costs.

A single management console allows administrators to manage the SourceOne system and control access to the archives. Organizational policies (or rules) created by administrators through this management console dictate the automated transfer of email, file, or Microsoft SharePoint data into archive folders. Various levels of privilege, assigned by folder, define who has access to the archived data. Reporting capabilities are also available to administrators through a Microsoft SQL[3] server web interface providing access to audit logs.

The EMC SourceOne product family includes the following products for the processing of email, file, and Microsoft SharePoint content:

- **EMC SourceOne Email Management** – archives email from Microsoft Exchange and IBM Lotus Domino mail servers, retaining pointers (shortcuts) to archived messages and attachments, making the action transparent to end users. EMC SourceOne for Email Management is the base application required for all other EMC SourceOne products.
- **EMC SourceOne for Microsoft SharePoint** – supports policy-based archiving of Microsoft SharePoint content into the EMC SourceOne archive to provide efficient storage of SharePoint content.
- **EMC SourceOne for File Systems** – supports file archiving with archiving policies based on data attributes such as age, file size, or file type with indexing of file metadata for efficient search and retrieval.

Additional capabilities beyond archiving are provided by adding the following EMC SourceOne product offerings to EMC SourceOne Email Management:

- **EMC SourceOne Discovery Manager** – enables legal discovery searches and secure legal hold[4] of archived content in response to legal and regulatory notices or corporate policy requests. Built around a legal matter metaphor, it enables authorized users to quickly find, review, and export archived information relevant to an inquiry.
- **EMC SourceOne Email Supervisor** – monitors email archives to comply with corporate policies and National Association of Securities Dealers (NASD) regulations.

1.3.1 EMC SourceOne Architecture

EMC SourceOne is built on a scalable, flexible, N+1[5] distributed system architecture that can support deployments of varying sizes from small business to enterprise. As mentioned earlier, EMC SourceOne Email Management provides the core architecture required to support all other EMC SourceOne products. The components of this core architecture encompassing applications, processing services, databases and archives are illustrated in Figure 1. Components that are part of the operational environment such as mail

[1] IBM – International Business Machines
[2] SMTP – Simple Mail Transfer Protocol
[3] SQL – Structured Query Language
[4] Legal hold – messages are saved in an EMC SourceOne hold folder with no retention period.
[5] N+1 – a type of redundancy whereby an additional spare item allows for normal operation in the event of a failure in one of N required items.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

and file data sources, EmailXtender[6], and storage, including file system, network-attached storage (NAS), storage area network (SAN), and other supported devices, are also illustrated in Figure 1. The previously unused acronym "IIS" in the illustration stands for Internet Information Services.

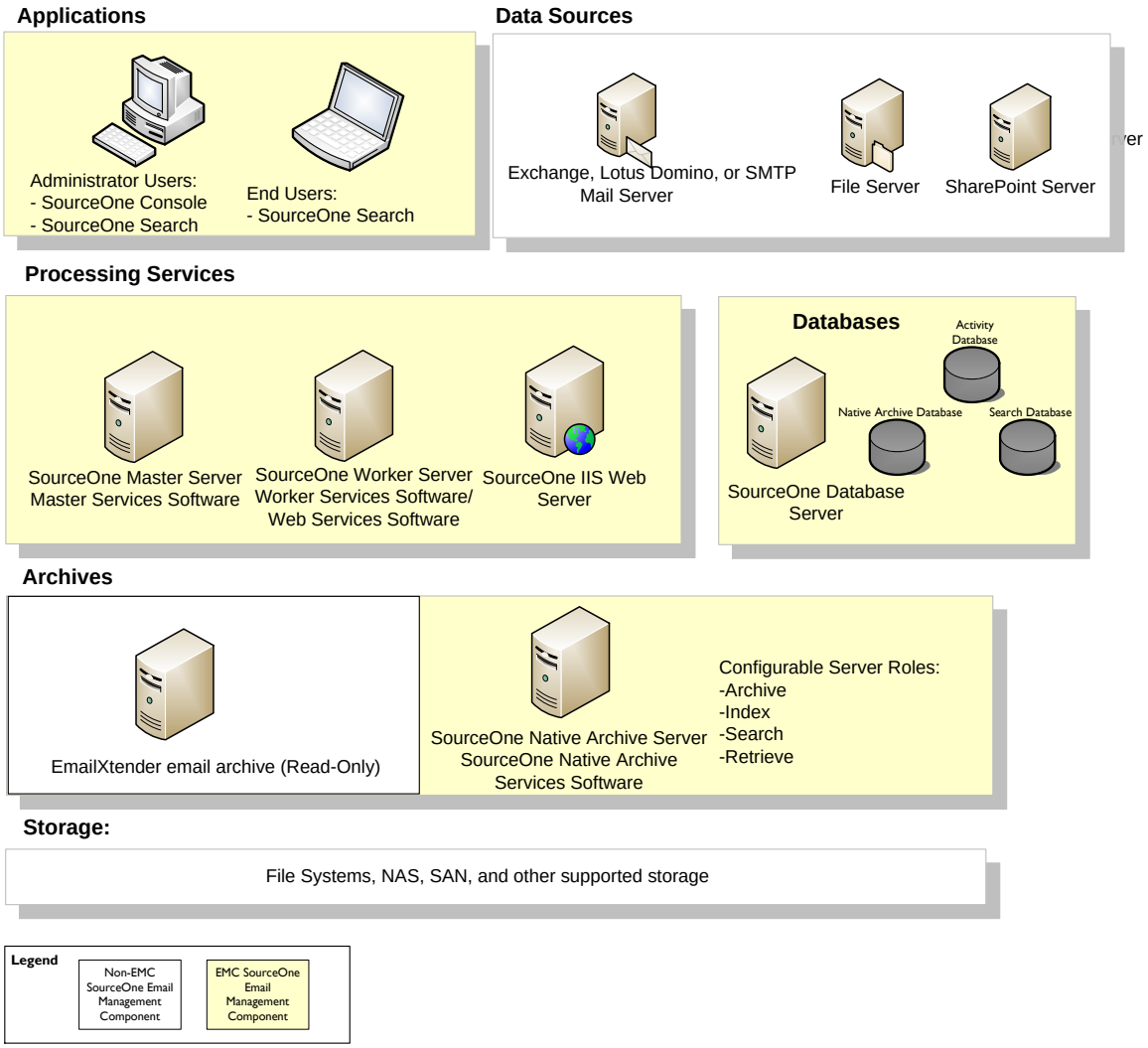

Figure 1 EMC SourceOne Core System Architecture

1.3.1.1 Applications

There are two primary EMC SourceOne Email Management applications: EMC SourceOne Console and EMC SourceOne Search.

The EMC SourceOne Console is a Microsoft Management Console (MMC) snap-in run from an administrator's desktop. It enables administrators to centrally configure and manage the EMC SourceOne system. Administrators are able to create archive folders; create mapped folders (which map folders in the user's environment to the archive folders); set permissions on these mapped folders to control access; and

[6] EmailXtender – an EMC precursor product to SourceOne.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

assign archiving activities (in discrete work units called "jobs") to computers called SourceOne Worker Servers for processing.

The EMC SourceOne Search application supports end user and administrative searches for archived email content through an intuitive web interface. SourceOne Search is typically installed on a SourceOne IIS Web server and securely communicates with Source One Web Services software installed on one or more Worker Server computers behind a firewall. It can also be installed directly on a Worker Server.

With EMC SourceOne Email Management, optional SourceOne Reporting software is also available to provide administrators with the capability to configure and view audit log reports.

1.3.1.2 Processing Services

The activities scheduled through the SourceOne Console are executed by the processing services provided by these SourceOne software components:

- Master Services software
- Worker Services software
- Web Services software

The SourceOne architecture is scalable, supporting the installation of all processing services on a single host computer or distributed across multiple host computers, depending on the requirements of the operational environment.

Master Services software running on SourceOne Master Servers schedules and distributes jobs for processing by Worker Services and monitors Worker Servers for failures. Worker Services processes jobs (e.g., ingesting email for archiving) from designated data sources. To balance the workload and prioritize jobs, each Worker Server can be configured to process up to 16 jobs simultaneously and be assigned only specific job types as needed. Worker Services assumes control of jobs based on the type of jobs it's assigned to process. With the add-on SourceOne products EMC SourceOne for Microsoft SharePoint and EMC SourceOne for File Systems, the Worker Servers can be configured to process SharePoint and file system related jobs, respectively.

Web Services software supports underlying Web functions such as those needed by SourceOne Search to provide the search web interface to end users and administrators. It also supports legal discovery operations with the add-on product EMC SourceOne Discovery Manager. The Web Services software is installed on one or more computers on which Worker Services software is also installed. This creates an IIS Web site (called "SearchWS").

The SourceOne system configuration, including activities requiring processing, is maintained in the SourceOne databases.

1.3.1.3 Databases

The following SourceOne databases are installed on a Microsoft SQL server to support EMC SourceOne Email Management:

- Activity database – maintains data associated with EMC SourceOne system processing as described in the section above.
- Native Archive database – manages data associated with the EMC SourceOne Native Archive, a role-based architecture that manages the archiving, indexing, searching, and retrieving of content.
- Search database – maintains data associated with the EMC SourceOne Search application.

An additional Discovery Manager database is installed with the add-on product EMC SourceOne Discovery Manager.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.3.1.4 Archives

EMC SourceOne supports two types of archives:

1. EMC SourceOne Native Archive
2. EmailXtender 4.8 Service Pack 1 email archive (read-only)

The EMC SourceOne Native Archive supports a role-based architecture whereby SourceOne Native Archive Services software can be installed on a single computer or multiple host computers to perform the following roles:

- Archive
- Index
- Search
- Retrieve

This role-based architecture enables an organization to dedicate hardware to specific roles as needed to match its archiving policies. For example, in small-to-medium business environments, the Native Archive Services software can perform all roles using one physical host computer. In enterprise environments, it can be installed and configured on multiple physical host computers that act as a single virtual computer.

Each archive folder on a SourceOne Native Archive Server is referred to as a native archive folder. These folders are connected to one or more storage environments to house the large amount of data archived by EMC SourceOne. The Native Archive Server also stores database and program disk data. File system, SAN, NAS, or a combination of these storage types are possible depending on the size and throughput requirements of the specific environment. Connectivity to the storage devices is provided using current device connectivity methods such as Fibre Channel or iSCSI[7] over Ethernet, depending on the type of storage environment being used. Supported storage from EMC includes Celerra, Centera, Atmos, and Data Domain. NetApp is also supported.

1.3.2 EMC SourceOne Methodology

Administrators configure the SourceOne system to archive content from various sources (i.e., email, file, or SharePoint servers). Once an activity is created, jobs associated with that activity execute on one or more Worker Servers within the SourceOne system. Information about activities and jobs is stored within the SourceOne Activity database. The following three steps summarize how EMC SourceOne archives content:

1. An activity is created by an EMC SourceOne administrator using the EMC SourceOne Console. An example of an activity would be a "Journaling" activity, which can be used to archive messages from a mail server.
2. Once an activity is created, the activity is stored in the SourceOne Activity database. Jobs are generated automatically to perform the work of the activity, and those jobs are stored in the SourceOne Activity database as well.
3. Periodically, SourceOne Worker Servers check the SourceOne Activity database for jobs they can perform (not all SourceOne Worker Servers may be configured to perform all jobs). If a matching job is found, that job is then run on the SourceOne Worker Server.

EMC SourceOne Email Management performs the following types of email archiving:

- Real-time archiving – also referred to as journaling, of messages from mail servers and drop directories into which SMTP mail is placed.
- Historical archiving – of messages from Microsoft Exchange mailboxes and PST[8] files and IBM Lotus mailboxes and NFS[9] files. Administrators can capture data from individual mailboxes and public folders on a scheduled basis.

[7] iSCSI – Internet Small Computer System Interface
[8] PST – Personal Storage Tables
[9] NFS – Network Files System

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- "User directed archiving" (UDA) – enables an email user or application to direct business important messages to a specific mapped folder in EMC SourceOne Email Management with set retention periods for archiving.

Once archived, content can be searched by administrators and end users as described in Section 1.3.1.1 using the EMC SourceOne Search application. With EMC SourceOne Discovery Manager, administrators can perform role-based searches for archived content; copy items to EMC SourceOne legal hold folders (configured using the EMC SourceOne Console) that are de-duplicated and full-text indexed; save searches for audit and re-use; and export items to PST, NSF, or Electronic Discovery Reference Model (EDRM) Extensible Markup Language (XML) format. EMC SourceOne Discovery Manager also maps multiple email addresses to a single identity record for accurate historical searching.

The EMC SourceOne software is supported on various Microsoft Windows operating systems (OSs), including Microsoft Windows 2003 Server and Microsoft Windows 2008 R2 Server. The EMC SourceOne platform is also certified as VMware ready, with options for running particular tasks or the entire solution in VMware sessions.

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 TOE, and defining the specific evaluated configuration.

The TOE is an email, file, and SharePoint archiving solution with web-based search capabilities, access control to archived content, auditing and reporting capabilities, and windows-based authentication. It is implemented as a collection of applications, processing services, databases, and archives running on Windows based systems.

1.4.1 TOE Components

The following components comprise the software-only TOE:

- SourceOne Email Management v7.2
  - SourceOne Console software
  - SourceOne Search software
  - SourceOne Master Services software
  - SourceOne Worker Services software
  - SourceOne Web Services software
  - SourceOne Native Archive Services software
  - SourceOne Reporting software
  - SourceOne Email Management database
- SourceOne for Microsoft SharePoint v7.1
  - SourceOne SharePoint Solutions software
  - SourceOne for Microsoft SharePoint Business Component Extensions (BCEs) software (installed on Worker Servers to enable processing of SharePoint activities and on computers hosting the SourceOne Console)
- SourceOne for File Systems v7.2
  - SourceOne for File Systems BCEs software
- SourceOne Discovery Manager v7.2
  - SourceOne Discovery Manager Server software
  - SourceOne Discovery Manager Client software
  - SourceOne Discovery Manager Web Client software
  - SourceOne Discovery Manager database

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Figure 2 shows the details of the deployment configuration of the TOE. The following previously undefined acronyms appear in Figure 2:

- AD – Active Directory
- CIFS – Common Internet File System
- DFS – Distributed File System

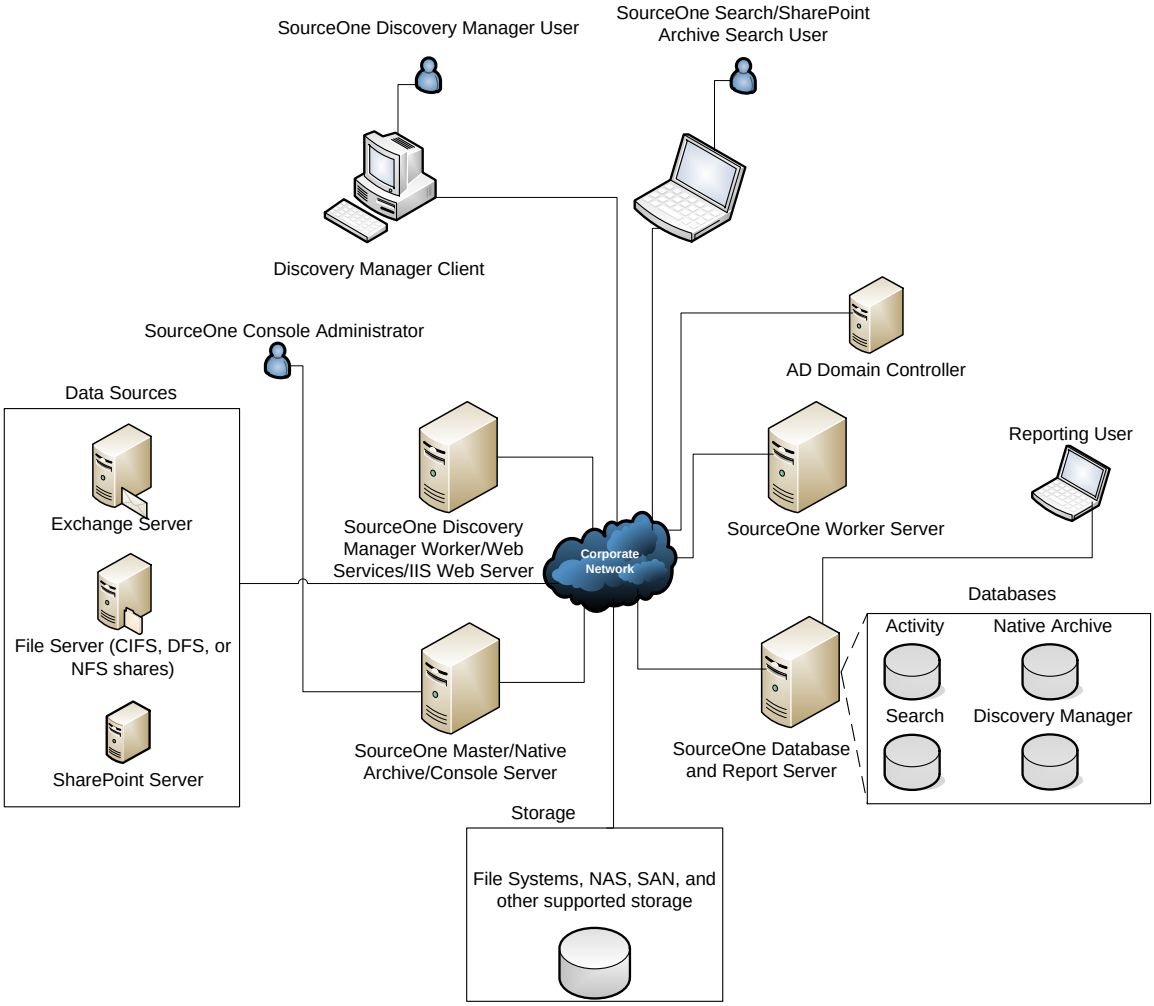

Figure 2 Deployment Configuration of the TOE

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.4.2 Brief Description of the Components of the TOE

The TOE consists of the following software components:

1.4.2.1 SourceOne Email Management

The following sections describe the components that comprise SourceOne Email Management.

1.4.2.1.1 SourceOne Console Software

The SourceOne Console software is a graphical user interface implemented as a MMC snap-in that allows SourceOne administrators authenticated with their Windows logon credentials to configure and manage the TOE. The SourceOne Console is used to do the following:

- Configure Native Archive folders and storage
- Configure SourceOne mapped folders (including user and group permissions)
- Create policies and activities that generate jobs for SourceOne Worker Servers
- Configure SourceOne Worker Servers (including the type and number of jobs allowed to run)
- Configure auditing for SourceOne Search operations. Auditing is always on for Discovery Manager search operations.

It includes a Job Distribution Framework (JDF) application programming interface (API) to the SourceOne Activity database where jobs are maintained.

1.4.2.1.2 SourceOne Search Software (SearchWS)

SourceOne Search software installed on a SourceOne IIS Web Server provides web-based archive search functionality. Users are authenticated with their Windows logon credentials (using forms-based authentication, as well as NTLM[10] or Kerberos in a single sign-on (SSO) configuration) and searches are authorized based on the type of search and the mapped folder permissions of the user invoking the search (assigned by a SourceOne administrator).

The SourceOne Search software installs an IIS Web site (Search) that is the user interface and passes query and results data over HTTPS with Transport Layer Security (TLS) to and from the SourceOne SearchWS Web site on a SourceOne Worker Server. HTTPS/TLS is also used between an end user's Web browser and the Search Web site. Note that cryptographic services are not included as part of the evaluation.

SourceOne Search is used to find archived content. SourceOne administrators can search for email content, files, and SharePoint content. End users can search for email content and files; however, they must use the SourceOne Archive Search (see Section 1.4.2.2.1) functionality integrated into the SharePoint Server to search archived SharePoint content for which they have permission to access. There are five types of searches that can be performed depending on a user's level of permissions:

- My files
- Administrator
- My Items
- My Contributed Items
- All Items

By default, end users do not have any SourceOne folder permissions to conduct searches. They must be explicitly granted such permissions by a SourceOne administrator. End users do have "Restore" capabilities by default. Restore is used to restore email messages to mailboxes on the mail server or file content to file systems. "Copy To (Archive)" functionality is reserved for users with Administrator folder permission only. This functionality is used to restore and copy selected archived email messages or file systems content to another archive folder. Messages may also be deleted from the archives with search types "Administrator" and "My Contributed Items". The Delete operation is available for the My Contributed Items search type

[10] NTLM – NT LAN Manager

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

only if the user invoking the operation has been given Delete permission on the mapped folders containing the message to be deleted. The Delete operation is not available for All Items, My Items, and My Files search types.

The mapped folders listed (available for a selected search type) are those for which a user has been granted appropriate permission. For example, to perform an Administrator search on a folder, a user must have Administrator permission on that folder. SourceOne legal hold folders are not available in SourceOne Search; instead they are accessed via SourceOne Discovery Manager.

Every search generates a job that is scheduled for execution on Worker Servers by SourceOne Master Services software as described below.

1.4.2.1.3 SourceOne Master Services Software

The SourceOne Master Services software schedules jobs and monitors workers. It includes a "Job Scheduler" wherein Job Business Services (JBSs) read the SourceOne Activity database and then schedule and distribute jobs (e.g., ingesting email from a mailbox) to the various SourceOne Worker Servers. The SourceOne Activity database is read through a JDF API.

1.4.2.1.4 SourceOne Worker Services Software

The jobs scheduled through the Master Server are executed on Worker Servers by the Worker Services software. Each Worker Server can process up to 16 jobs at a time. Jobs are processed through Job Business Components (JBCs) and augmented with plug-in code called Business Component Extensions (BCEs) for file system and SharePoint archiving. The SourceOne Worker Services software uses secure Remote Procedure Call (RPC) for communication with the SourceOne Native Archive. (EmailXtender is not part of the evaluated configuration).

The SourceOne Worker Services software implements a Job dispatcher service that "pulls" scheduled jobs based upon available capacity allowing balancing across the SourceOne Worker Servers in an optimal fashion. Having jobs scheduled across any of the SourceOne Worker Servers allows the elimination of a static binding between any single SourceOne Worker Server and a source of data. Instead, the TOE shares a single configuration (maintained by the SourceOne Activity database) across the entire system and processes data in a distributed manner.

1.4.2.1.5 SourceOne Web Services Software

The SourceOne Web Services software is provided over a secure HTTPS/TLS path to SourceOne Search on the SourceOne IIS Web Server and supports other SourceOne web-based applications directly like SourceOne Discovery Manager. Note that cryptographic services are not included as part of the evaluation.

1.4.2.1.6 SourceOne Native Archive Services Software

The SourceOne Native Archive Services software performs four roles: archive server, index server, search server, and retrieval server.

- Archive server – archives content sent over RPC from a Worker Server JBC. It also communicates indexing requirements to the Index server.
- Index server – performs archive data full-text indexing.
- Search server – processes SourceOne Search and SourceOne Discovery Manager operations, communicating over RPC to SourceOne Web Services running on SourceOne Worker Servers and Discovery Manager Worker Servers, respectively.
- Retrieval server – performs archive retrieval from search or shortcut recall operations, communicating with SourceOne Web Services over RPC.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.4.2.1.7 SourceOne Reporting Software

The TOE uses Microsoft SQL Server Reporting Services (SSRS) to generate audit reports of search operations performed using SourceOne Search, changes to user permissions on mapped folders, and all SourceOne Discovery Manager operations.

For SourceOne Search operations and changes to mapped folder permissions, audit information is stored in the SourceOne Activity database. For the following SourceOne Discovery Manager operations, audit information is stored in the SourceOne Discovery Manager database:

- Collection searches
- Assign to matter with hold folder
- Delete from matter with hold folder
- Exports

The SourceOne Discovery Manager operations are always audited. No auditing configuration is required.

SourceOne Reporting provides two sets of reports:

- SourceOne reports – includes Search Audit reports for SourceOne Search, Configuration reports, and System reports.
- Discovery Manager reports – includes Search Audit reports for SourceOne Discovery Manager collection searches, assign to hold folder operations, delete from hold folder operations, documents viewed, and exports.

SourceOne Reporting uses role based access control (RBAC) to control access to the audit logs. Authorized users authenticated with their Windows logon credentials use Internet Explorer 7 or higher on a client computer to access the SourceOne Reporting SSRS web site and run SourceOne reports. Adobe Acrobat Reader is used to view and print reports in PDF[11] format. SSRS is used by an authorized administrator to assign users to different roles. The Content Manager role and the Browser role have pre-defined permissions in SSRS.

1.4.2.1.8 SourceOne Databases

The SourceOne Activity, Search, and Native Archive databases are installed on the Database and Report Server to process SourceOne activities; manage SourceOne Search; and manage archiving, indexing, searching, and retrieving. The SourceOne database install lays down the data structures of these databases; however, the physical data files themselves are stored in the TOE environment.

1.4.2.1.9 SourceOne Discovery Manager Client Software

The SourceOne Discovery Manager Client software provides a thick client user interface for authorized administrators as well as other authorized users to administer and search the archives for legal discovery. RBAC is employed to segregate SourceOne Discovery Manager operations to specific individuals as configured by an authorized administrator using the SourceOne Discovery Manager Client.

1.4.2.1.10 SourceOne Discovery Manager Web Client Software

The SourceOne Discovery Manager Web Client software installed on a SourceOne ISS Web Server provides a web-based interface for authorized administrators as well as other authorized users to administer and search the archives for legal discovery. As with the Discovery Manager thick client user interface, RBAC is employed to segregate SourceOne Discovery Manager operations to specific individuals as configured by an authorized administrator using either the SourceOne Discovery Manager Client or Web Client.

Users are authenticated with their Windows logon credentials using forms-based authentication and authorization of a user's role is performed on every search or export request.

[11] PDF – Portable Document Format

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.4.2.2 SourceOne for Microsoft SharePoint

SourceOne for Microsoft SharePoint functionality, including administration, archiving, search, and restore, are provided by SharePoint solutions (contained in .wsp files) and BCEs. The SharePoint solutions are installed on SharePoint Central Administration or web front-end (WFE) servers in the SharePoint environment. The BCEs are installed on Worker Servers and the computer hosting the SourceOne Console. These components are described below.

1.4.2.2.1 SharePoint Solutions

There are two types of SharePoint solutions deployed.

- Central Administration web applications – These solutions deploy custom administration sites for configuring SourceOne for Microsoft SharePoint features in SharePoint. They are installed on a server hosting the Central Administration site.
- Content web applications – These solutions deploy the web applications to support the SourceOne for Microsoft SharePoint features. They are installed on WFE servers in the SharePoint environment.

Three content web application solutions are installed:

- SharePoint Archive – activates a service that provides the SourceOne archiving functionality for Microsoft SharePoint.
- SharePoint Archive Search – provides the SourceOne archive search functionality for Microsoft SharePoint. It provides a template and web parts that a SourceOne administrator uses to create an Archive Search site integrated into SharePoint. Using this site, end users can find, preview, and download content archived through SharePoint Archive. SharePoint Archive Search only searches for archived SharePoint content from the current farm. It relies on SourceOne SearchWS and Web Services, and access is restricted using AD for authentication. Permissions are controlled based on the SharePoint group/AD group/AD user association a user had at the time the content was archived. End users do not need permissions on mapped folder to use the SharePoint Archive Search site.
- SharePoint Archive Search Restore – provides the SourceOne Archive Search Restore functionality for Microsoft SharePoint.

1.4.2.2.2 SourceOne for Microsoft SharePoint BCE Software

SourceOne for Microsoft SharePoint BCE software provides SharePoint archiving and restore functionality on the SourceOne Worker Server and computer hosting the SourceOne Console. The BCEs allow the SourceOne administrator to use the SourceOne Console to configure SharePoint activities that are processed by the SourceOne Worker Servers.

1.4.2.3 SourceOne for File Systems

SourceOne for File Systems BCE software provides file archiving functionality on the SourceOne Worker Server and computer hosting the SourceOne Console. It allows for file archiving from CIFS, DFS, and NFS shares.

1.4.2.4 SourceOne Discovery Manager

SourceOne Discovery Manager is based on a client server architecture.

1.4.2.4.1 SourceOne Discovery Manager Server Software

The SourceOne Discovery Manager Server software uses Model View Controller (MVC) and Simple Object Access Protocol (SOAP). Installing this software along with SourceOne Web Services on a Worker Server provides a Discovery Manager Web service (IIS Web site called "Discovery Manager"). This Web service schedules the execution of several operations on behalf of the Discovery Manager Client and Web Client software, including discovery searches and copying results to a legal hold folder.

1.4.2.4.2 SourceOne Discovery Manager Client Software

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

The SourceOne Discovery Manager Client software is a thick client that provides a user interface to perform discovery tasks based on the roles assigned to a user. SourceOne Discovery Manager Client performs all authentication and authorization based on Windows logon credentials. The SourceOne Discovery Manager Client software disables or hides functions for which a user does not have permissions. Authorization information (database permissions) is stored in Microsoft SQL. Default and matter-specific roles are supported. The Discovery Manager Client communicates with the Discovery Manager Server over HTTPS/TLS. Note that cryptographic services are not included as part of the evaluation.

The Discovery Manager Client software is installed on a standard desktop or laptop used in a corporate environment.

1.4.2.4.3 SourceOne Discovery Manager Web Client Software

The SourceOne Discovery Manager Web Client software is a web based interface that provides a user interface to perform discovery tasks based on the roles assigned to a user. SourceOne Discovery Manager Web Client performs all authentication and authorization based on Windows logon credentials. The SourceOne Discovery Manager Web Client software disables or hides functions for which a user does not have permissions. Authorization information (database permissions) is stored in Microsoft SQL. Default and matter-specific roles are supported. The Discovery Manager Web Client communicates with the Discovery Manager Server over HTTPS/TLS. Note that cryptographic services are not included as part of the evaluation.

1.4.2.4.4 SourceOne Discovery Manager Database

The SourceOne Discovery Manager database is installed on the Database and Report Server to process SourceOne Discovery Manager operations. The SourceOne Discovery Manager database install lays down the data structures of this database; however, the physical data files themselves are stored in the TOE environment.

1.4.3 TOE Environment

In the evaluated configuration, all of the TOE software components are running on Windows-based platforms within a virtualized environment provided by VMware ESXi 5.0.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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

Table 2 TOE Minimum Requirements

Category	Requirement
SourceOne Worker Server	
Software	Microsoft .NET Framework 4.0 Redistributable Package Microsoft Outlook 2010
OS	Microsoft Windows Server 2008 R2 SP1, Standard or Enterprise edition, (64-bit)
Hardware/Hypervisor	VMware ESXi 5.0 Minimum 2 CPUs[12], 4GB[13] memory, 1Gbps[14] network, and 32 GB of local hard disk
SourceOne Master/Native Archive/Console Server	
Software	Microsoft .NET Framework 4.0 Redistributable Package MMC 3.0 (for SourceOne Console) Internet Control Message Protocol enabled
OS	Same as Worker Server
Hardware/Hypervisor	VMware ESXi 5.0 Same as Worker Server plus 20 GB of free space on local drive for indexing
SourceOne Database and Report Server	
Software	Microsoft SQL Server 2008 R2 SP1, Standard or Enterprise License Microsoft SQL Server 2008 R2 SP2 Reporting Service
OS	Microsoft Windows Server 2008 R2 SP1, Standard or Enterprise edition, (64-bit)
Hardware/Hypervisor	VMware ESXi 5.0 Minimum 4 CPUs and 8 GB memory
SourceOne Discovery Manager Worker/Web Services/IIS Web Server	
Software	SourceOne Discovery Manager Server software must be installed on a SourceOne Worker Server on which SourceOne Web Services software is also installed. Microsoft.NET Framework 4.0 Redistributable Package Microsoft Outlook 2010 Microsoft ASP.NET and Microsoft IIS
OS	Same as Worker Server
Hardware/Hypervisor	VMware ESXi 5.0 Same as Worker Server
SourceOne Reporting Client	
OS	Microsoft Windows 7 SP1
Browser	Internet Explorer 7.0 or higher
Software	Adobe Acrobat Reader to view and print SourceOne reports in PDF format Minimum screen resolution of 1024x768 for standard size monitors, or the equivalent for wide-screen monitors
Hardware	Standard desktop or laptop used in a corporate environment

[12] CPU – Central Processing Unit
[13] GB – Gigabyte
[14] Gbps – Gigabits per second

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Category	Requirement
Discovery Manager Client	
Software	Microsoft Outlook 2010, 32-bit or 64-bit Microsoft.NET Framework 4.0 Redistributable Package
OS	Microsoft Windows 7 SP1, Home or Professional edition or Ultimate edition, 32-bit or 64-bit
Hardware/Hypervisor	VMware ESXi 5.0 Standard hardware requirements for a typical desktop or laptop used in a corporate environment Minimum computer display setting 800x600
Network	Standard connection to the corporate network
Network	
Authentication servers	AD Domain Controller provided by Microsoft Windows 2008 R2
Network	High-speed connection to all components and systems in the configuration with sufficient bandwidth to process the expected workload
Other Environmental Components	
Storage Devices	A storage environment is required to store the large amount of data archived by SourceOne as well as databases, logs, program disk data, and other configuration data. Supported storage types include file systems, SAN, NAS, or a combination, depending on the size and throughput requirements of the specific environment. Connectivity to the storage devices can be provided using current device connectivity methods such as Fibre Channel or iSCSI over Ethernet, depending on the type of storage environment being used. EMC devices (Atmos/Celerra/Centera/Data Domain/Symmetrix) and NetApp devices are supported.
Microsoft Exchange	Microsoft Exchange Server 2010
Microsoft SharePoint	Microsoft SharePoint Server 2010 initial release Required on all SharePoint WFE servers - Microsoft Visual C++ 2010 Redistributable Package (x86) The browsers used to access SourceOne Archive Search: • Must be supported by SharePoint • Must have JavaScript enabled

1.5 TOE Description

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

1.5.1 Physical Scope

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

The TOE is a software-only email, file, and SharePoint archiving solution running on Virtual Machines (VMs) with the minimum software and hardware requirements as listed in Table 2. The TOE is installed on a network and can have numerous deployment scenarios since it presents a distributed architecture. The processing services software components are designed to run on one or more VMs depending on the requirements of the operational environment. Figure 3 illustrates a basic configuration of the TOE and

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

represents the evaluated configuration for the purposes of CC testing. All of the TOE software components shown in Figure 3 must be installed for the TOE to be in the evaluated configuration.

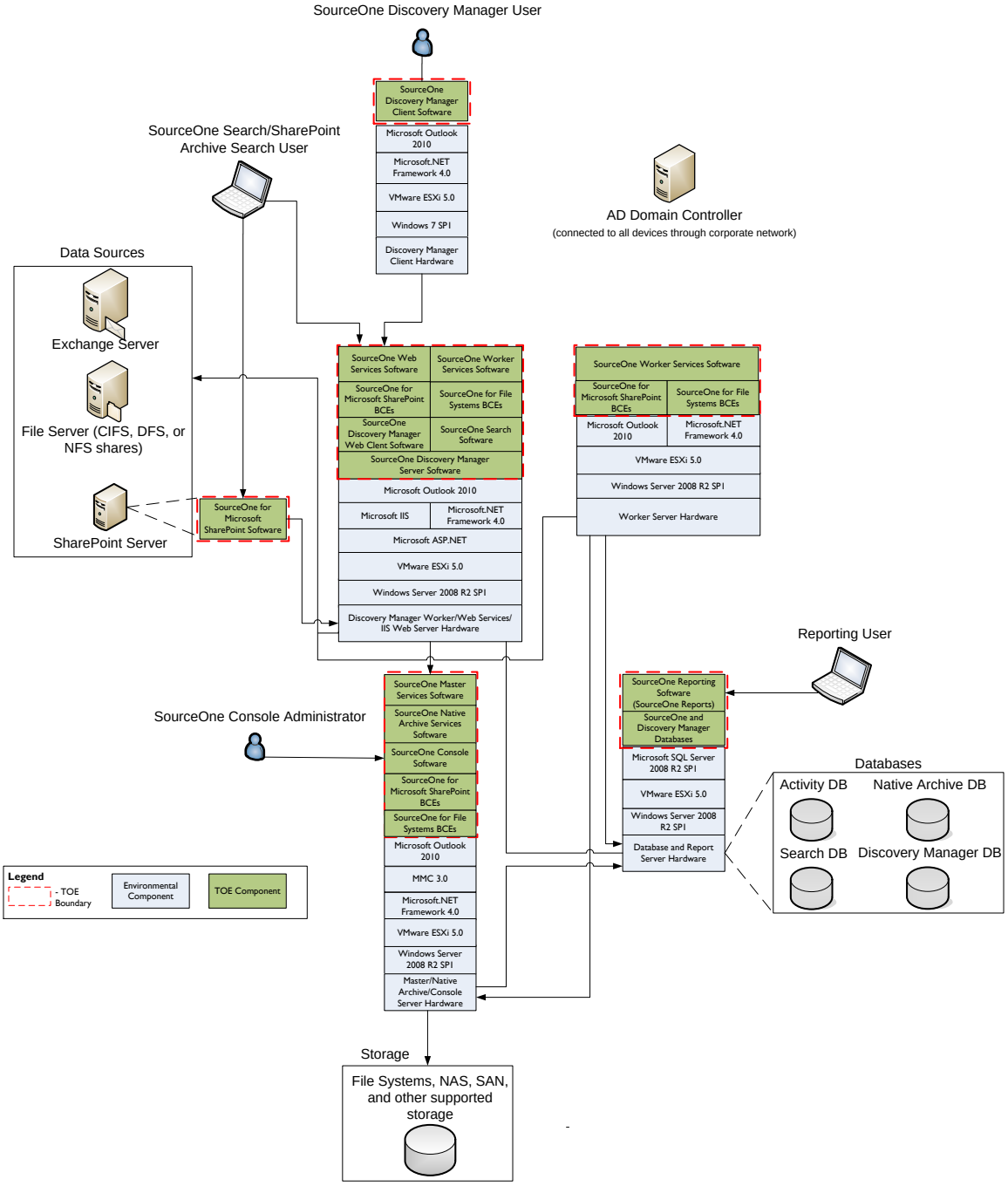

Figure 3 Physical TOE Boundary

In the evaluated configuration, the Source One Discovery Manager Worker/Web Services/IIS Web Server, Master/Native Archive/Console Server, Worker Server, and Database and Report Server operate with Windows Server 2008 R2 SP1. The Discovery Manager client host computer is a standard laptop or desktop with Windows 7 SP1. The evaluated configuration also includes Microsoft Exchange Server 2010 and SharePoint Server 2010.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

The TOE boundary includes the TOE software components depicted as such in Figure 3. It does not include licensable application modules such as those that facilitate integration with Microsoft IIS, Microsoft SQL, Microsoft SSRS, Microsoft Exchange, and Microsoft SharePoint, or any external storage systems. It also does not include the browsers, the underlying operating systems, hardware platforms, and communication infrastructure.

1.5.1.1 TOE Software

The TOE is a software-only email, file, and SharePoint archiving solution consisting of the components illustrated in Figure 3 and listed below:

- SourceOne Email Management v7.2
  - SourceOne Console software
  - SourceOne Search software
  - SourceOne Master Services software
  - SourceOne Worker Services software
  - SourceOne Web Service software
  - SourceOne Native Archive Services software
  - SourceOne Reporting software
  - SourceOne Databases
  - SourceOne Discovery Manager Client software (automatically installed with SourceOne Email Management)
- SourceOne for Microsoft SharePoint v7.1
  - SourceOne SharePoint Solutions
  - SourceOne for Microsoft SharePoint BCEs software
- SourceOne for File Systems v7.2
  - SourceOne for File Systems BCEs software
- SourceOne Discovery Manager v7.2
  - SourceOne Discovery Manager Client software
  - SourceOne Discovery Manager Web Client software
  - SourceOne Discovery Manager Server software
  - SourceOne Discovery Manager Database

1.5.1.2 Guidance Documentation

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

- EMC SourceOne Email Management 7.2 Installation Guide
- EMC SourceOne Email Management 7.2 Administration Guide
- EMC SourceOne 7.2 Search User Guide
- EMC SourceOne Products Compatibility Guide
- EMC SourceOne Email Management 7.2 Release Notes
- EMC SourceOne Discovery Manager 7.2 Installation and Administration Guide
- EMC SourceOne Discovery Manager 7.2 Desktop User Guide
- EMC SourceOne Discovery Manager 7.2 Web Application User Guide
- EMC SourceOne Discovery Manager 7.2 Release Notes
- EMC SourceOne for Microsoft SharePoint 7.1 Installation Guide
- EMC SourceOne for Microsoft SharePoint 7.1 Administration Guide
- EMC SourceOne 7.2 for File Systems Administration Guide
- EMC SourceOne for File Systems, Version 7.2, Installation Guide
- EMC SourceOne for File Systems 7.2 Release Notes
- EMC SourceOne 7.2 Auditing and Reporting Installation and Administration Guide

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes 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 usefully grouped under the following Security Function Classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functions
- Resource Utilization

1.5.2.1 Security Audit

The TOE generates audit records for SourceOne Search operations and for changes to user permissions on mapped folders. Audit information is stored in the SourceOne Activity databases. For SourceOne Discovery Manager, the TOE also generates audit records for collection searches, documents viewed, assign to matter with hold folder operations, delete from matter with hold folder operations, and exports. This audit information is stored in the SourceOne Discovery Manager database.

While some audit events may be configured for SourceOne Search operations (including specifying specific users to be audited), all SourceOne Discovery Manager events are audited by default. Audit information is viewed in SourceOne reports and Discovery Manager reports available to authorized users through SourceOne Reporting.

1.5.2.2 User Data Protection

The TOE enforces SourceOne mapped folder and RBAC access control SFP[15]s, which dictate the operations subjects may perform based on a set of security attributes. Subjects of the SFP include SourceOne Search, Discovery Manager, and SharePoint Archive Search users and SourceOne Console Administrators.

All operations on SourceOne mapped folders by SourceOne Search users as well as Discovery Manager Matter Managers are restricted based on a user's mapped folder permissions as assigned by SourceOne administrators. SharePoint Archive Search users are restricted access to mapped folders based on group membership (all AD and SharePoint groups to which the user belongs).

The RBAC access control SFP restricts access to the Discovery Manager Client and Web Client user interface and the SourceOne Console based on a user's role. The SourceOne Discovery Manager Client and Web Client will disable or hide functions for which a user does not have permissions. Global and Matter specific roles are supported.

The SourceOne RBAC access control SFP ensures that only SourceOne Console Administrators can use the SourceOne Console to create activities that control the import of email, file, and SharePoint content for archiving. Through these activities, they define the archive criteria, such as the data sources, activity types, mapped folders, rules, and filters.

Authorized SourceOne Discovery Manager users may export archived content and associated metadata (i.e., information about a message, such as its subject, received date, or sender) in EDRM XML format. The SourceOne RBAC access control SFP ensures that only users in the Investigator role have privileges to run exports.

[15] SFP – Security Function Policy

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

For exports of user data, the SourceOne mapped folder access control SFP is enforced allowing SourceOne Search and SharePoint Archive Search users to restore only archive content for which they have permissions on the associated SourceOne mapped folders.

1.5.2.3 Identification and Authentication

The TOE maintains several security attributes, other than user ID[16], on an individual basis that are used to enforce the SFRs, including mapped folder permission and roles. All users must be identified and authenticated with their Windows Logon credentials prior to performing any action on the TOE.

1.5.2.4 Security Management

Security Management functions define how the security functionality of the TOE is managed, the roles that are authorized to perform management functions, and the management of attributes that dictate the security functionality.

The SourceOne Console is the primary management interface for the TOE. It provides several functions for managing SourceOne resources, such as creating mapped folders and assigning permission to those folders and configuring Worker Servers. SourceOne Console Administrators are provided access to the SourceOne Console to perform these tasks.

The Discovery Manager Client and Web Client provide the following roles for administration: Discovery Manager User Administrator, Discovery Manager Application Administrator, Discovery Manager Tag Administrator, Discovery Manager Identity Administrator, and Backup Operator. Several user roles are also supported.

Reporting Services includes the following roles for configuring and viewing audit reports: Browser and Content Manager roles.

The mapped folder permissions and roles assigned to users are restrictive by default. Only authorized administrators are able to make changes to these security attributes. The SourceOne Console Administrator maintains the mapped folder permissions. In the Discovery Manager Client and Web Client application, the User Administrator selects users from AD. These users are added to the Discovery Manager database. Only users that are listed in the Discovery Manager database can use the client application.

1.5.2.5 Protection of the TSF

The TOE is capable of recovering from Worker Server failures based on its N+1 and stateless architecture. If this server fails, the load can be picked up by another server of the same type.

1.5.2.6 Resource Utilization

The TOE provides resource allocation by allowing SourceOne Console Administrators to limit the number of jobs performed simultaneously on any Worker Server. The SourceOne Console Administrator can also prioritize jobs by assigning only specific jobs to each Worker Server.

The TOE provides limited fault tolerance in the event of a Worker Server failure. TOE operation continues normally as a server of the same type takes over the processing of the failed machine.

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

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

- Physical hardware implementation (the TOE running on physical hardware versus virtual hardware as provided by a VMware environment)

[16] ID – Identifier

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- Supported Windows OSs other than those listed in Table 2
- EMC SourceOne Email Supervisor
- EmailXtender
- DiskXtender
- SMTP and IBM Lotus Domino mail environments
- EMC SourceOne Mobile Services software
- EMC SourceOne for Microsoft SharePoint Storage Management
- SharePoint Online (cloud-based environments)
- SharePoint External Blob Storage components
- Discovery Manager Express Edition
- EMC SourceOne Offline Access

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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, Release 4, September 2012; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2014/05/06 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented with Flaw Reporting Procedures (ALC_FLR.2)

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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[17] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

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

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[18] 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.MASQUERADE	A non-TOE user may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.TAMPERING	A non-TOE user may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.
T.UNAUTH	A TOE user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security function policy.
T.MONOPOLIZE	A TOE user or process acting on behalf of that user may monopolize TOE resources preventing important task from completing.

3.2 Organizational Security Policies

An OSP is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no OSPs imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration.

[17] IT – Information Technology
[18] TSF – TOE Security Functionality

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 5 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 5 Assumptions

Name	Description
A.INSTALL	The TOE is installed on the appropriate, dedicated hardware and operating system.
A.NETCON	The TOE environment provides the network connectivity required to allow the TOE to perform its functions.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.
A.LOCATE	The TOE is located within a controlled access facility.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 6 below.

Table 6 Security Objectives for the TOE

Name	Description
O.AUDIT	The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to select audit events and review the audit trail.
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.
O.AUTHENTICATE	The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
O.PROTECT	The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.
O.RESOURCES	The TOE must protect against resource monopolization by providing mechanisms to limit use of available resources.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 7 below lists the IT security objectives that are to be satisfied by the environment.

Table 7 IT Security Objectives

Name	Description
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.PLATFORM	The TOE hardware and OS must support all required TOE functions.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description
OE.NETWORK	The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.

4.2.2 Non-IT Security Objectives

Table 8 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 8 Non-IT Security Objectives

Name	Description
OE.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.
OE.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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

There are no extended TOE security functional components defined for this evaluation.

5.2 Extended TOE Security Assurance Components

There are no extended TOE security assurance components defined for this evaluation.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 9 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓	✓	
FAU_SAR.1	Audit review		✓		
FAU_SEL.1	Selective audit	✓	✓		
FDP_ACC.1 (a)	Subset access control		✓		✓
FDP_ACC.1 (b)	Subset access control		✓		✓
FDP_ACF.1 (a)	Security attribute based access control		✓		✓
FDP_ACF.1 (b)	Security attribute based access control		✓		✓
FDP_ETC.2	Export of user data with security attributes		✓		
FDP_ITC.1	Import of user data without security attributes		✓		
FIA_ATD.1	User attribute definition		✓		
FIA_UAU.2	User authentication before any action				
FIA_UID.2	User identification before any action				
FMT_MSA.1 (a)	Management of security attributes	✓	✓		✓
FMT_MSA.1 (b)	Management of security attributes	✓	✓		✓

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	S	A	R	I
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_FLS.1	Failure with preservation of secure state		✓		
FRU_FLT.2	Limited fault tolerance		✓		
FRU_PRS.1	Limited priority of service		✓		
FRU_RSA.1	Maximum quotas	✓	✓		

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

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation
Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps
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) [*changes to user permissions on mapped folders;*
d) all SourceOne Search operations performed using the Administrator search type;
e) SourceOne Search operations performed using the My Items, My contributed Items, or All Items search types by audited users (as explicitly identified via LDAP query); and
f) the following Discovery Manager operations: all collection searches; documents viewed; collection search results assigned to a matter with a hold folder (copied to the hold folder); collection search results deleted from a matter with a hold folder (deleted from the hold folder); and exports].

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 information*].

Application Note: The TSF is comprised of several components that are registered as Windows services, and therefore the TOE start-up and shutdown events are captured in the Windows Event Log.

Application Note: A matter is another term for an investigation or case. A hold folder is a SourceOne Legal Hold folder where copies of messages are retained to prevent them from being deleted when their retention expires. Hold folders are used to retain messages found during a collection search for the lifetime of the matter.

FAU_SAR.1 Audit review
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FAU_SAR.1.1

The TSF shall provide [*Browser role, Content Manager role*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2

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

FAU_SEL.1 Selective audit
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data
FAU_SEL.1.1

The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) [user identity]
b) [*type of search operation*].

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.2 Class FDP: User Data Protection

FDP_ACC.1(a) Subset access control
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1

The TSF shall enforce the [*SourceOne mapped folder access control SFP*] on [

- *Subjects:*
  - *SourceOne Search users*
  - *SharePoint Archive Search users*
  - *Discovery Manager Matter Manager users*
- *Objects: SourceOne mapped folders*
- *Operations:*
  - *For SourceOne Search users (end users and SourceOne administrators) - all searches of archived content associated with mapped folders, including restores of archived content back to original data source,*
  - *For SharePoint Archive Search users – all searches of archived SharePoint content, including restores of data to the SharePoint data source*
  - *For Discovery Manager Matter Manager users – choose folders to add to matter*].

FDP_ACC.1(b) Subset access control
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1

The TSF shall enforce the [*SourceOne RBAC access control SFP*] on [

- *Subjects: SourceOne Console Administrators and SourceOne Discovery Manager users (all roles)*
- *Objects: Discovery Manager Client and Web Client user interface and SourceOne Console*
- *Operations:*
  a. *For SourceOne Console Administrators – all activities created through SourceOne Console resulting in import of data into the TOE,*
  b. *For SourceOne Discovery Manager users (all roles) – all interactions with the Discovery Manager Client or Web Client user interface, including export operations (limited to users in Investigator role).*].

FDP_ACF.1(a) Security attribute based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1

The TSF shall enforce the [*SourceOne mapped folder access control SFP*] to objects based on the following: [

- *Subject attributes:*
  - *For SourceOne Search users - mapped folder permissions and ownership or permission on the archived item, defined through user/group ID*
  - *For SharePoint Archive Search users – group membership (all AD and SharePoint groups to which the user belongs)*
  - *For Discovery Manager Matter Manager users – mapped folder permissions*
- *Object attributes: type of mapped folder, To/From/Cc/Bcc line on archived email, ACL on archived files from file server, AD and SharePoint group association on archived SharePoint content.*].

FDP_ACF.1.2

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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

- *if a SourceOne Search user has permissions on a mapped folder, then the user is given access to the mapped folder according to the rules defined in Table 10;*
- *if a SourceOne Discovery Manager Matter Manager user has "Matter Manager Access" permission on a mapped folder, then the user is given all access to the mapped folder.*
- *if a SourceOne SharePoint Archive Search user's group membership matches the AD and SharePoint group permissions on the SharePoint archived content in a mapped folder, then the user is permitted to perform all searches on this archived SharePoint content, including restores of data to the SharePoint server.*].

Table 10 Mapped Folder Access Control Rules

Mapped Folder Permissions (Subject)	Mapped Folder Type (Object)	Rules Governing Access to Mapped Folders
Owner	Organizational, Community or Personal (mail content)	• Can see only email items for which he has ownership* (My Items search). • Can restore email messages to own mailbox • Cannot delete items from the folder. *Ownership defined as follows: • For journaled email messages in Organization mapped folders – all senders and receivers (internal and external), i.e., subjects whose user/group ID matches object's To/From/Cc/Bcc line. • For journaled email messages in Personal and Community mapped folders – internal recipients, i.e., subjects whose user/group ID matches the object's To or BCC line. • For messages archived through historical and PST archiving, or UDA, only mailbox or mail file owners are set as message owners.
Contributor	Community or Personal (email content)	• User can read only the email items that he directed to be archived into a UDA folder, or those for which he has ownership and were journaled or archived into a Personal or Community mapped folder (My Contributed Items search). • User can restore email messages to own mailbox

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Mapped Folder Permissions (Subject)	Mapped Folder Type (Object)	Rules Governing Access to Mapped Folders
My Files	Organization (file content)	• User can see only files for which he has access permission (files originally owned by the user on the file system, as determined by a match of the subject's user/group ID to the file ACL or as specified by a Console Administrator in the file archive activity (My Files search). • User can restore file to its original location. • User cannot delete items from the folder.
Read All	Organization, Community and Personal	• Can see all items in the folder, even if he is not the owner of the email items or does not have access permission to the files or SharePoint items (All Items search). • Has read-only privileges on all items in the folder. • Cannot delete items from the folder
Administrator	Organization, Community and Personal	• Has full control over all items in the folder (Administrator search) • Can search, retrieve, and delete items in the folder. • Can restore files to their original location. • Can restore email messages to another user's mailbox. • Can search for all archived content types (email, files, SharePoint).
Delete	Community and Personal	• Can delete the email items that he directed to be archived into a UDA folder, or that were journaled or archived into a Personal or Community mapped folder.

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [*none*].

FDP_ACF.1(b) Security attribute based access control

Hierarchical to: No other components.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Dependencies: **FDP_ACC.1 Subset access control**
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1

The TSF shall enforce the [*SourceOne RBAC access control SFP*] to objects based on the following: [

- *Subject attributes: Role*
- *Object attributes: None*].

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 a subject requests access to an object and the role associated with that subject has permission to access that object, then access is granted.*
- *otherwise access is denied.]*.

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [*none*].

FDP_ETC.2 Export of user data with security attributes

Hierarchical to: **No other components.**
Dependencies: **[FDP_ACC.1 Subset access control, or**
FDP_IFC.1 Subset information flow control]

FDP_ETC.2.1

The TSF shall enforce the [*SourceOne mapped folder and RBAC access control SFPs*] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2

The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3

The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4

The TSF shall enforce the following rules when user data is exported from the TOE: [*no additional exportation control rules*].

FDP_ITC.1 Import of user data without security attributes

Hierarchical to: **No other components.**
Dependencies: **[FDP_ACC.1 Subset access control, or**
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1

The TSF shall enforce the [*SourceOne RBAC access control SFP*] when importing user data, 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: [*no additional importation control rules*].

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.3 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition
Hierarchical to: No other components.
Dependencies: No dependencies
FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [

- *Permissions on mapped folders*
- *Discovery Manager username and AD security identifier (SID) – stored in Discovery Manager database*
- *Discovery Manager role assignment*
- *Identity records (all of the addresses or email addresses for a particular user*].

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification
FIA_UAU.2.1

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

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies
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.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.4 Class FMT: Security Management

FMT_MSA.1 (a) Management of security attributes
Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1

The TSF shall enforce the [*SourceOne mapped folder access control SFP*] to restrict the ability to [query, modify, delete, [*select*]] the security attributes [*user and group map folder permissions*] to [*SourceOne Console Administrator*].

FMT_MSA.1 (b) Management of security attributes
Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1

The TSF shall enforce the [*SourceOne RBAC access control SFP*] to restrict the ability to [change_default, query, modify, delete] the security attributes [SourceOne Discovery Manager *roles*] to [*authorized administrators*].

FMT_MSA.3 Static attribute initialisation
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1

The TSF shall enforce the [*SourceOne mapped folder and RBAC access control SFPs*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*SourceOne Console Administrator, SourceOne Discovery Manager User Administrator*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data
Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1

The TSF shall restrict the ability to [[*perform the operations listed in Table 11*]] to the [*TSF data listed in Table 11*] to [*the roles listed in Table 11*].

Table 11 Management of TSF Data

Operation	TSF Data	Role
SourceOne Console		
Assign/Unassign	Windows Users, Windows Groups, and LDAP Query Groups	Console Administrator or SourceOne Administrator (defined through Primary Service account)

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Operation	TSF Data	Role
Create, Modify, and Delete	Policies, activities, and rules	Console Administrator
Create and Delete	Native Archive folders	Console Administrator
View, Create, Modify, Copy, and Delete	SourceOne mapped folders	Console Administrator
Assign, modify, delete	User and group permissions on mapped folders	Console Administrator
Modify	Native Archive folder properties	Console Administrator
View, edit	Worker properties	Console Administrator
Specify	Users to be audited ("audited users")	Console Administrator
Select	Events to be audited	Console Administrator
SourceOne Discovery Manager		
Add users, remove users, assign roles	Discovery Manager users and roles	Discovery Manager User Administrator
Configure	Discovery Manager settings	Discovery Manager Application Administrator
Create, Modify, and Delete	Identity Records	Discovery Manager Identity Administrator
SourceOne Reporting		
View and Customize	Audit reports	Content Manager
View	Audit reports	Browser role

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components.
Dependencies: No Dependencies
FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [*SourceOne Console management; SourceOne Reporting (audit) management; authentication data management; SourceOne Discovery Manager management]*.

FMT_SMR.1 Security roles
Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification
FMT_SMR.1.1

The TSF shall maintain the roles {

a. *For SourceOne Console: Console Administrator (supported by TOE through Admins group with the Console Administrator account)*
b. *For SourceOne Discovery Manager: Application Administrator, User Administrator, Identity Administrator, Tag Administrator, Backup Operator, Matter Owner, Matter Manager, and Investigator*
c. *For SourceOne Reporting: Content Manager and Browser*

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

d. *For SourceOne: SourceOne Administrator (supported by TOE through Security group with Primary Service account)}.*

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.5 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state
Hierarchical to: No other components.
Dependencies: No dependencies.
FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [*Worker Server failures*].

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.6 Class FRU: Resource Utilization

FRU_FLT.2 Limited fault tolerance
Hierarchical to: FRU_FLT.1 Degraded fault tolerance
Dependencies: FPT_FLS.1 Failure with preservation of secure state
FRU_FLT.2.1
The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: [*Worker Server failure*].

FRU_PRS.1 Limited priority of service
Hierarchical to: No other components.
Dependencies: No dependencies
FRU_PRS.1.1
The TSF shall assign a priority to each subject in the TSF.
FRU_PRS.1.2
The TSF shall ensure that each access to [*Worker Servers*] shall be mediated on the basis of the subjects assigned priority.

Application Note: The subjects referred to by this SFR are jobs of a particular type.

FRU_RSA.1 Maximum quotas
Hierarchical to: No other components.
Dependencies: No dependencies
FRU_RSA.1.1
The TSF shall enforce maximum quotas of the following resources: [*Worker Server processing capability*] that [subjects] can use [simultaneously].

Application Note: The subjects referred to by this SFR are jobs of a particular type.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 12 Assurance Requirements summarizes the requirements.

Table 12 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 Analysis of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

7 TOE Security 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 Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 13 lists the security functionality and their associated SFRs.

Table 13 Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit review
	FAU_SEL.1	Selective audit
User Data Protection	FDP_ACC.1 (a)	Subset access control
	FDP_ACC.1 (b)	Subset access control
	FDP_ACF.1 (a)	Security attribute based access control
	FDP_ACF.1 (b)	Security attribute based access control
	FDP_ETC.2	Export of user data with security attributes
	FDP_ITC.1	Import of user data without security attributes
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MSA.1 (a)	Management of security attributes
	FMT_MSA.1 (b)	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of TOE Security Functions	FPT_FLS.1	Failure with preservation of secure state
Resource Utilization	FRU_FLT.2	Limited fault tolerance

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

TOE Security Functionality	SFR ID	Description
	FRU_PRS.1	Limited priority of service
	FRU_RSA.1	Maximum quotas

7.1.1 Security Audit

The TOE generates audit records for SourceOne Search operations and changes to user permissions on mapped folders. This audit information is stored in the SourceOne Activity database. Similarly, for SourceOne Discovery Manager, the TOE generates audit records for collection searches, documents viewed, assign to matter with hold folder operations, delete from matter with hold folder operations, and exports. Audit information for SourceOne Discovery Manager is stored in the SourceOne Discovery Manager database.

While some audit events may be configured for SourceOne Search, all SourceOne Discovery Manager events are audited by default. Audit information is provided in SourceOne reports and Discovery Manager reports. These reports can be viewed only by users in the Browser and Content Manager role using the SourceOne Reporting application.

The audit information is provided in multiple reports as follows:

- Search Audit reports – these provide the audit information for SourceOne Search operations:
  - Search Activity, Search Copy, Search Delete, Search Restore, Documents Copied, Documents Deleted, Documents Restored, Documents Viewed
- Configuration reports – these provide the audit information for changes to user permissions on mapped folders:
  - Mapped Folder Permissions Audit, Mapped Folder Effective Permissions
- Discovery Manager reports – these provide the audit information for Discovery Manager:
  - Search Activity, Assign to Hold Folder, Delete from Hold Folder, Documents Viewed, Export Activity

The start-up and shut down events of the TOE are provided with the support of the TOE environment. Each TOE processing service is registered as a Windows service, and start-up/shutdown events are stored in the Windows Event Log. The Windows Event Log is viewed by authorized administrators using the Microsoft Windows Event Viewer.

Using SSRS, authorized administrators set permissions for users to access the SourceOne and Discovery Manager reports by assigning groups or users to different roles and setting database read and write permissions. The default Content Manager and Browser role have the following pre-defined permissions:

- Content Manager – view and customize reports, assigned to the SourceOne Security Group defined in AD.
- Browser – read-only access to reports, assigned to a report users group created by SourceOne Administrators in AD. The report users group would typically contain administrators, legal users, and compliance officers.

SourceOne Console Administrators select the set of events to be audited during TOE operation, including specific users to be audited and the type of search operation. Administrator and Discovery Manager events are audited by default.

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

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

7.1.2 User Data Protection

The TOE enforces the SourceOne mapped folder and RBAC access control SFPs, which dictate the operations subjects may perform based on a set of security attributes. Subjects of the SFP include SourceOne Search users (end users and SourceOne Administrators), Discovery Manager users (all roles), and SharePoint Archive Search users.

All operations on SourceOne mapped folders by SourceOne Search and Discovery Manager Matter Managers are restricted based on a user's mapped folder permissions assigned by the SourceOne Console Administrator. Besides mapped folder permissions, for SourceOne Search users the Windows User ID also establishes a user's ownership on the archived content, which varies by content type. For email ownership, a match is made to the To/From/Cc/Bcc line; for file ownership, the Access Control List is used. If a SourceOne Search users permissions on a mapped folder are removed, the user will still be able to access previous search results (view and perform a restore on email items) for a default period of 7 days. The user will not, however, be able to perform new searches or downloads against the associated mapped folder. The Console Administrator can reduce the number of calendar days (down to one) to save search results for users using the **Application Configuration** menu in the SourceOne Console.

SharePoint Archive Search users are restricted access to mapped folders based on group membership (all AD and SharePoint groups to which the user belongs). When the SharePoint Archive activity archives a SharePoint item, the item is stamped with the AD and SharePoint groups that have access to the item. SourceOne stores the group information. When a user logs in to the SharePoint Archive Search site, SourceOne determines the user's groups:

- All Active Directory groups to which the user belongs
- All SharePoint groups to which the user belongs on the current farm

When a user runs an Archive Search, results are constrained based on the user's group membership.

The RBAC access control policy restricts access to the Discovery Manager Client and Web Client user interface and the SourceOne Console based on a user's role. The SourceOne Discovery Manager Client and Web Client will disable or hide functions for which a user does not have permissions. Global and Matter specific roles are supported. Authorized SourceOne Discovery Manager users may export archived content and associated metadata in EDRM XML format. Only users in the Investigator role have privileges to run exports.

The RBAC access control SFP ensures that only SourceOne Console Administrators can use the SourceOne Console to create activities that control the import of email, file, and SharePoint content for archiving. When a SourceOne Console Administrator creates activities, rules are selected that determine the content to be processed by the activity. Email management activities can be configured to do the following:

- journal and archive email in real-time
- archive email from selected mailboxes and PST files, based on a schedule
- shortcut messages by replacing archived messages on a mail server with shortcuts to those messages in the SourceOne Native Archive
- archive items stored in UDA folders

Both the SourceOne mapped folder and RBAC access control SFPs are enforced when exporting user data outside of the TOE. The SourceOne mapped folder access control SFP is enforced when exporting user data by ensuring that SourceOne Search users have the appropriate mapped folder permissions before allowing that user to restore archived content back to the original data source (export). If the rules are satisfied to grant the user access to the mapped folders, then restores are permitted.

The SourceOne mapped folder access control SFP is also enforced when exporting user data by ensuring that SourceOne SharePoint Archive Search user's group membership matches the AD and SharePoint group permissions on the SharePoint archived content before allowing the user to restore archived data to the SharePoint server.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Finally, the SourceOne RBAC access control SFP is enforced when exporting user data by ensuring that only users in the Investigator role can perform exports in SourceOne Discovery Manager.
TOE Security Functional Requirements Satisfied: FDP_ACC.1 (a), FDP_ACC.1 (b), FDP_ACF.1 (a), FDP_ACF.1 (b), FDP_ETC.2, FDP_ITC.1

7.1.3 Identification and Authentication

The TOE maintains several security attributes, other than user ID, on an individual basis that are used to enforce the SFRs. These include the following:

- Permissions on mapped folders
- Discovery Manager username and AD security identifier (SID) – stored in Discovery Manager database
- Discovery Manager role assignment
- Identity records (all of the addresses or email addresses for a particular user)

Identification and authentication functions deal with how a user's identity is asserted and subsequently verified by the TOE. The TOE supports external authentication, which allows the TOE to validate a user's Windows logon credentials against AD.

When users access the SourceOne Console, Discovery Manager Client or Web Client, SourceOne Search, SharePoint Archive Search, or SourceOne Reporting service, their Windows logon credentials are passed to AD for verification. Users must be identified and authenticated with their Windows Logon credentials prior to performing any action on the TOE.

In addition to authentication, AD is used for authorization of SourceOne Console Administrators and SourceOne Reporting users. The TOE maintains a set of security roles, to which it maps a set of external roles, or AD accounts and groups. Subjects are bound to the security role for which an association has been established with an external role. If a user is not a member of any of the associated external roles, the SourceOne Console and Reporting service deny the user access. Once a user is authenticated, they must possess the appropriate privilege to perform any operations associated with these functions.

For Discovery Manager, the TOE uses the SIDs and role assignments maintained in the Discovery Manager database to determine authorizations, after authentication has been performed.

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

7.1.4 Security Management

Security Management functions define how the security functionality of the TOE is managed, the roles that are authorized to perform management functions, and the management of attributes that dictate the security functionality.

The SourceOne Console is the primary management interface for the TOE. It provides several functions for SourceOne Console Administrators to manage SourceOne resources:

- Creating policies, activities, and rules
- Managing user and group permissions on mapped folders
- Setting Native Archive folder properties
- Configuring Worker Servers
- Configuring audit events

The TOE authorizes access to the SourceOne Console based on the administrator's Windows Logon credentials, in particular their assignment to specific AD user accounts and groups. The SourceOne Console Administrators are assigned to the EMC SourceOne Admins group.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

The SourceOne Discovery Manager Client and Web Client include the following roles for administration:

- Discovery Manager User Administrator – adds users and assigns roles.
- Discovery Manager Application Administrator – manages the Discovery Manager application.
- Discovery Manager Tag Administrator – creates tags that are available to all matters. Investigators apply tags to specific items collected for the matter, to label the items for further review.
- Discovery Manager Identity Administrator – creates aliases (identity records) that simplify searching email. Each identity record contains all of the email addresses for a particular person of interest (custodian).
- Backup Operator – Performs SourceOne Discovery Manager backups.

In SourceOne Discovery Manager, roles control access to a matter (investigation) and define the actions a user can perform on a matter during its lifecycle. User roles include the following:

- Matter Owner – creates matters, by default becoming the first Matter Manager and Investigator in the matter, and can assign other Matter Managers and Investigators.
- Matter Managers
    - Assign and remove Matter Managers and Investigators to the matter
    - Specify and modify matter properties
    - Monitor progress and status of the matter
    - Close the matter
    - Reopen the matter
    - Delete the matter (Matter Managers must also have the Matter Owner role to delete matters.)
- Investigator
    - Collect, review, and export within the matter
    - Delete items from the matter
    - Apply and remove tags

SourceOne Reporting users are assigned one of the following roles: Browser and Content Manager roles. Both of these roles can read information from the audit records (reports). The Content Manager role can also customize audit reports.

SourceOne Search and SharePoint Archive Search users are not assigned roles.

The mapped folder permissions and roles assigned to users are restrictive by default. Only authorized administrators are able to make changes to these security attributes. The SourceOne Console Administrator maintains the mapped folder permissions. In the Discovery Manager Client and Web Client application, the User Administrator selects users from AD and assigns roles. These users are added to the Discovery Manager database. Only users that are listed in the Discovery Manager database can use the Discovery Manager Client and Web Client application. The User Administrator must specify individual users, not groups or distribution lists. When users are added to the Discovery Manager database, the name of the user and their SID from AD are stored in the Discovery Manager database. A Primary Service account user creates the first Discovery Manager user (User Administrator) with all roles at installation.

The TOE provides for audit management by allowing SourceOne Console Administrators to select the set of events to be audited during TOE operation, including specific users to be audited and the type of search operation. It also allows SourceOne Reporting users to customize reports.

TOE Security Functional Requirements Satisfied: FMT_MSA.1(a), FMT_MSA.1(b), FMS_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

7.1.5 Protection of the TSF

The TOE is capable of recovering from Worker Server failures based on its N+1 and stateless architecture. If a Worker Server fails, the load can be picked up by another server of the same type. In the evaluated configuration, the load will be picked up by the Discovery Manager Worker Server.

TOE Security Functional Requirements Satisfied: FPT_FLS.1

7.1.6 Resource Utilization

The TOE monitors the processes on SourceOne Worker Servers and a "heartbeat" sent from them to ensure that they are working properly. In the event of a Worker Server failure, the SourceOne Master Server can stop execution of jobs that are not successful and reschedule them to allow them to be picked up by another Worker Server and thereby ensure operation of all the TOE's capabilities

The TOE provides resource allocation by allowing SourceOne Console Administrators to limit the number of jobs of a certain job type performed simultaneously on any SourceOne Worker Server. Higher priority job types will be allowed to run more jobs simultaneously. By putting quotas on the maximum number of jobs of a certain job type that can be processed on any Worker Server simultaneously, the TOE prevents jobs from monopolizing the Worker Server resources. A Worker Server will only process the maximum number of job instances of a particular job type simultaneously as specified by a SourceOne Console Administrator in the Worker Server properties.

The SourceOne Console Administrator can also prioritize jobs by assigning only specific job types to each SourceOne Worker Server. A Console Administrator determines a jobs priority. Access to Worker Server processing capability is based on this priority. Higher priority job types are given more access by assigning them dedicated Worker Servers (Worker Servers configured to only process jobs of a certain job type) or allowing a higher number of jobs of a certain job type to run simultaneously on any Worker Server. Worker Servers will only pull jobs from the Activity database that match the job type and limit they've been assigned. This ensures that Worker Server processing is allocated to the more important jobs, and cannot be monopolized by lower priority jobs.

The TOE provides limited fault tolerance in the event of a Worker Server failure. TOE operation continues normally as a server of the same type takes over the processing of the failed machine.

TOE Security Functional Requirements Satisfied: FRU_RSA.1, FRU_PRS.1, FRU_FLT.1

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 Release 4.

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 0 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 14 below provides a mapping of the objectives to the threats they counter.

Table 14 Threats: Objectives Mapping

Threats	Objectives	Rationale
T.MASQUERADE A non-TOE user may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	By ensuring that the TOE is able to identify and authenticate users prior to allowing access to TOE administrative functions and data, O.AUTHENTICATE satisfies this threat.
T.TAMPERING A non-TOE user may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.	O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to select audit events and review the audit trail.	The objective O.AUDIT ensures that security relevant events that may indicate attempts to tamper with the TOE are recorded.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges 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 security mechanisms.
	O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	O.PROTECT mitigates this threat by providing mechanisms to protect the TOE data from unauthorized modification.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Threats	Objectives	Rationale
T.UNAUTH A TOE user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security function policy.	O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to select audit events and review the audit trail.	The objective O.AUDIT ensures that Administrator and audited user access to the TOE data is recorded.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges 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.
	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	The objective O.AUTHENTICATE ensures that users are identified and authenticated prior to gaining access to TOE security data.
T.MONOPOLIZE A TOE user or process acting on behalf of that user may monopolize TOE resources preventing important task from completing.	O.RESOURCES The TOE must protect against resource monopolization by providing mechanisms to limit use of available resources.	By ensuring that the TOE is able to limit resource use on Worker Servers, O.RESOURCES satisfies this threat.

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

8.2.2 Security Objectives Rationale Relating to Policies

There are no Organizational Security Policies defined for this Security Target.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 15 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 15 Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL The TOE is installed on the appropriate, dedicated hardware and operating system.	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.
	OE.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. OE.MANAGE satisfies this assumption.
A.NETCON The TOE environment provides the network connectivity required to allow the TOE to perform its functions.	OE.NETWORK The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.	OE.NETWORK satisfies the assumption that the TOE environment will provide the appropriate connectivity to allow the TOE to perform its function.
A.TIMESTAMP The IT environment provides the TOE 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.LOCATE The TOE is located within a controlled access facility.	OE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	Physical security is provided within the TOE environment to provide appropriate protection to the network resources. OE.PHYSICAL satisfies this assumption.
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.	The TOE environment provides protection from external interference or tampering. OE.PROTECT satisfies this assumption.
	OE.PLATFORM The TOE hardware and OS must support all required TOE functions.	The hardware and OS on which the TOE software runs provide a platform to prevent unauthorized modification of TOE software.
	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE	OE.MANAGE satisfies the assumption that the TOE software will be protected from unauthorized modification as users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Assumptions	Objectives	Rationale
	administrators will ensure the system is used securely.	
	OE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	Physical security is provided within the TOE environment to prevent unauthorized modification of TOE software. OE.PHYSICAL satisfies this assumption.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.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.	OE.MANAGE satisfies the assumption that competent individuals are assigned to manage the TOE and the TSF.
A.NOEVIL The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	OE.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.	OE.MANAGE satisfies the assumption that the users who manage the TOE are non-hostile, appropriately trained and follow all guidance.

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

There are no extended Security Functional Requirements in this ST.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended TOE Security Assurance Requirements in this ST.

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

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 16 Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	FIA_ATD.1 User attribute definition	The requirement meets the objective by storing role assignments that isolate administration tasks to users with appropriate privileges.
	FMT_MSA.1 (a) Management of security attributes	The requirement meets the objective by ensuring that only authorized administrators can manage security attributes (mapped folder permissions).
	FMT_MSA.1 (b) Management of security attributes	The requirement meets the objective by ensuring that only authorized administrators can manage security attributes (roles).
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by ensuring that security attributes are given restrictive values, and that only authorized users may provide alternative default values.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that the TOE restricts access to TSF management functions and data to authorized roles.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to select audit events and review the audit trail.	FAU_GEN.1 Audit Data Generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides the ability to review logs.
	FAU_SEL.1 Selective audit	The requirement meets the objective by ensuring that the TOE

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Objective	Requirements Addressing the Objective	Rationale
		provides authorized administrators the ability to select audit events to be audited.
O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that the users are authenticated before any TSF mediated access to the TOE functions or TSF data is allowed.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the users are identified before any TSF mediated access to the TOE functions or TSF data is allowed.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that only authorized users are allowed access to TSF data.
O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	FDP_ACC.1 (a) Subset access control	The requirement meets the objective by ensuring that mapped folder access control is applied to all actions requested by a user involving access to archived content.
	FDP_ACC.1 (b) Subset access control	The requirement meets the objective by ensuring that RBAC is applied to all actions requested by SourceOne Discovery Manager user (all roles) and the SourceOne Console Administrator.
	FDP_ACF.1 (a) Security attribute based access control	The requirement meets the objective by ensuring that the TOE enforces access control based on the implemented policy mapped folders).
	FDP_ACF.1 (b) Security attribute based access control	The requirement meets the objective by ensuring that the TOE enforces access control based on the implemented policy (RBAC).
	FDP_ETC.2 Export of user data with security attributes	This requirement meets the objective by ensuring only TOE users with the proper privileges and permissions may export data.
	FDP_ITC.1 Import of user data without security attributes	This requirement meets the objective by ensuring only the SourceOne Console

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Objective	Requirements Addressing the Objective	Rationale
		Administrator may import data content for archiving.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only authorized users have access to TSF data.
	FPT_FLS.1 Failure with preservation of secure state	The requirement meets the objective by ensuring that the TOE is capable of returning to a secure state if a failure condition occurs.
	FRU_FLT.2 Limited fault tolerance	The requirement meets the objective by ensuring that the TOE provides mechanisms for continued operation after Worker Server failures.
O.RESOURCES The TOE must protect against resource monopolization by providing mechanisms to limit use of available resources.	FRU_PRS.1 Limited priority of service	The requirement meets the objective by providing Console Administrators the ability to set priorities of service based on job type.
	FRU_RSA.1 Maximum quotas	The requirement meets the objective by providing administrators the ability to set job limits on Worker Servers.

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. The TOE 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 TOE 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 17 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.

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 17 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1		The OS is part of the TOE environment, thus accurate timestamps are provided by the TOE environment. This dependency is met instead by OE.TIME.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SEL.1	FAU_GEN.1	✓	
	FMT_MTD.1	✓	
FDP_ACC.1 (a)	FDP_ACF.1 (a)	✓	
FDP_ACC.1 (b)	FDP_ACF.1 (b)	✓	
FDP_ACF.1 (a)	FMT_MSA.3	✓	
	FDP_ACC.1 (a)	✓	
FDP_ACF.1 (b)	FDP_ACC.1 (b)	✓	
	FMT_MSA.3	✓	
FDP_ETC.2	FDP_ACC.1 (a)	✓	
	FDP_ACC.1 (b)	✓	
FDP_ITC.1	FDP_ACC.1 (b)	✓	
	FMT_MSA.3	✓	
FIA_ATD.1	No dependencies	✓	
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. This satisfies this dependency.
FIA_UID.2	No dependencies	✓	
FMT_MSA.1 (a)	FDP_ACC.1 (a)	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1 (b)	FDP_ACC.1 (b)	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

SFR ID	Dependencies	Dependency Met	Rationale
FMT_MTD.1	FMT_SMR.1	✓	
	FMT_SMF.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.2	FPT_FLS.1	✓	
FRU_PRS.1	No dependencies	✓	
FRU_RSA.1	No dependencies	✓	

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

9 Acronyms

Table 18 defines the acronyms used throughout this document.

Table 18 Acronyms

Acronym	Definition
AD	Active Directory
API	Application Programming Interface
BCE	Business Component Extension
CC	Common Criteria
CIFS	Common Internet File System
CPU	Central Processing Unit
DFS	Distributed File System
EAL	Evaluation Assurance Level
EDRM	Electronic Discovery Reference Model
GB	Gigabyte
Gbps	Gigabits per second
HTTPS	Hypertext Transfer Protocol Secure
IBM	International Business Machines
ID	Identifier
IIS	Internet Information Services
iSCSI	Internet Small Computer System Interface
IT	Information Technology
JBC	Job Business Component
JBS	Job Business Service
JDF	Job Distribution Framework
LDAP	Lightweight Directory Access Protocol
MMC	Microsoft Management Console
NAS	Network Attached Storage
NASD	National Association of Securities Dealers
NFS	Network File System
NTLM	NT LAN Manager
OS	Operating System
OSP	Organizational Security Policy
PDF	Portable Document Format

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Acronym	Definition
PP	Protection Profile
PST	Personal Storage Table
RBAC	Role Based Access Control
RPC	Remote Procedure Call
SAN	Storage Attached Network
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SID	Security Identifier
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSO	Single Sign-On
SSRS	SQL Server Reporting Services
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UDA	User Directed Archiving
VM	Virtual Machine
WFE	Web Front-End
XML	Extensible Markup Language

© 2016 EMC Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Prepared by:
Corsec Security, Inc.

13921 Park Center Road
Suite 460
Herndon, VA 20171
United States of America

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