Varonis Systems, Inc.

Data Governance Suite v6.2.38.0 including DataPrivilege v6.0.113

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.5

Prepared for:

VARONIS

Varonis Systems, Inc.
1250 Broadway
31st Floor
New York, NY 10001
United States of America

Phone: +1 877 292 8767
www.varonis.com

Prepared by:

Corsec

Corsec Security, Inc.
13921 Park Center Road
Suite 460
Herndon, VA 20171
United States of America

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

Table of Contents

List of Figures

List of Tables

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is the Varonis Systems, Inc. (Varonis) Data Governance Suite v6.2.38.0 including DataPrivilege v6.0.113 and will hereafter be referred to as DGS, or the TOE, throughout this document. The TOE is a file system access control management, auditing, and reporting system. The TOE tracks and records permissions used for file systems including those used in Windows, Linux/Unix, Directory Services, Exchange, SharePoint, and EMC or NetApp network attached storage devices. The system uses an agent-based architecture that tracks usage and permissions across a distributed network of computers and servers.

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 and Terms (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	Varonis Systems, Inc. Data Governance Suite v6.2.38.0 including DataPrivilege v6.0.113 Security Target
ST Version	Version 1.5
ST Author	Corsec Security, Inc.

ST Title	Varonis Systems, Inc. Data Governance Suite v6.2.38.0 including DataPrivilege v6.0.113 Security Target
ST Publication Date	2016-10-12
TOE Reference	Varonis Data Governance Suite v6.2.38.0 including DataPrivilege v6.0.113 • DatAdvantage v6.2.38.0 • DataPrivilege v6.0.113 • IDU Classification Framework v6.2.35.57 • DatAlert v6.2.35.57 • Data Transport Engine v6.2.35.57 • Probe v6.2.35.57 • Collector v6.2.35.57 • DatAdvantage UI v6.2.35.57 • DatAdvantage Management Console v6.2.35.57 • Powershell API v6.2.35.57 • Exchange Agent v5.9.68.5 • Windows Agent v6.2.35.57 • Unix Agent v6.2.181 • SharePoint Agent v6.2.35.57 • Directory Services Agent v6.2.35.57

1.3 TOE Overview

The TOE Overview summarizes the usage and major security features of the DGS. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type and describing the TOE.

The TOE is a suite of software applications that work with file systems across a network to audit, analyze, and remediate improper or insecure access permissions. The TOE works with a variety of different objects, including files, folders, Exchange mailboxes, Active Directories, and SharePoint sites and lists[1]. The primary components of the TOE included in the evaluation are:

- DatAdvantage
- DataPrivilege
- IDU[2] Classification Framework
- DatAlert
- Data Transport Engine

Additionally, the TOE includes the following interfaces:

- DatAdvantage User Interface (UI)
- DatAdvantage Management Console
- DataPrivilege
- PowerShell Application Programming Interface (API)

More information on these components and interfaces is provided below.

[1] These will be collectively referred to as “objects” throughout the remainder of this document.

[2] IDU – Intelligent Data Usage

1.3.1 DataAdvantage

DatAdvantage is the core component of the TOE. This application scans systems in order to locate objects and identify the end users[3] that have permission to access each object on the monitored systems. DatAdvantage then allows TOE users and administrators to use this information to view each object and list all of the end users with access to it, or view each end user and determine all of the objects that the end user can access. This is referred to as bidirectional permissions view.

DatAdvantage monitors remote systems by deploying agents, which are small processes that run in the background of the Operating System (OS) on monitored systems to monitor object access and permission changes in real time. In instances where agents cannot be deployed (systems without an open architecture OS), DatAdvantage uses probes, which are small programs that gather object access and permission changes from across the network. Probes store data in a small data store called a shadow database and require one shadow database for each monitored system. To support the operation of probes, sometimes an optional component that extends the functionality of the probes across separate networks, known as a collector, is deployed. A collector sits between the monitored machine and the probe, usually on a separate network, and relays object access and permission changes back to the probe. This can be useful in firewalled environments where the protocols used by DatAdvantage probes are blocked. Agents, probes, and collectors can work with Windows filesystems, Unix filesystems, Exchange mailboxes and public folders, Active Directories, and SharePoint shares. Probes and collectors alone can work with Network Attached Storage (NAS) devices, since these run on a fixed OS that does not allow an agent to be installed.

The TOE gathers data that indicates when an object is accessed, who accessed the object, and the nature of the access. The TOE also separately gathers permission data directly from objects. The TOE can look at this data to analyze permissions and access patterns and determine the set of end users that actually need access to each object and the permissions that can be safely removed. Removing extraneous permissions can prevent data from being overexposed, which could lead to misuse or data theft.

All permissions can be changed from within the DatAdvantage UI, a Windows-based graphical client interface that provides the analysis and permission control functionality for the TOE. Users and administrators can simulate changes before committing them in order to see how the changes will affect the end users who currently access the file. For example, if “Everyone” permissions are removed from a file, there may be non-obvious effects that result, such as end users who use the data no longer being permitted to do so. These cases can be discovered and remediated without causing any disruption to end users due to the simulation capabilities that DatAdvantage provides.

By analyzing access patterns to objects, DatAdvantage can help identify who is the “owner” of each object. Owners are the end user or group of end users who access the object most frequently.

1.3.2 DataPrivilege

DataPrivilege provides a web interface portal and automated tools for end users and data owners. The portal provides a set of graphical tools that data owners can use to see information about who has access to their data, who has been using their data, statistics about usage of their data, and the capability to control access to their

[3] End users are the users who access objects. Users or TOE users are the users who use the TOE functionality.

data. This offloads the work of managing file access from Information Technology (IT) departments and gives control to the people who actually own and use the data.

The DataPrivilege portal also provides a web form that end users who need access to data can fill out. The request is then sent to the data owner or owners, who can authorize or deny the access request. If authorized, DataPrivilege automatically makes the permission changes to the object and revokes them when access is no longer needed.

DataPrivilege can automate end user entitlement reviews by sending emails on a set schedule (e.g., every six months, every year, every quarter, etc.). These emails give a summary of the objects that the end user no longer uses and recommends that the access is revoked. The end user can agree to authorize the changes, which are then made automatically, or the end user can prevent the revocation of access by specifying that the change should not happen. This happens at a granular level, so end users can specify the folders or groups that they still need to access while allowing the system to remove their access to objects they no longer need.

The final functionality provided by DataPrivilege is the ability to set up "ethical walls". This refers to the ability to control access to objects such that two sets of users who shouldn't have access to the same data cannot both access it. This is useful if businesses want to separate data by department, or if there are instances where there would be a conflict of interest if two separate groups had access to the same information.

The DataPrivilege Interface is a web-based graphical UI that runs on an Internet Information Services (IIS) web server. This interface leverages existing IDU functionality to provide data owners with the capability to manage their data without requiring TOE users and administrators to micromanage the process.

1.3.3 IDU Classification Framework

The IDU Classification Framework identifies:

- the systems that store sensitive data (credit card info, health care information, social security numbers, etc.)
- the end users who can access that data
- the end users who have accessed that data recently
- what type of access was initiated
- the end user that owns the data
- where the data is overexposed

IDU Classification Framework in conjunction with DatAdvantage provides reporting on where sensitive data is most concentrated and allows prioritization of remediation efforts to restrict access to sensitive data where it may exist in an insecure state.

By making use of real-time monitoring, IDU Classification Framework with DatAdvantage allows users to see sensitive data as soon as it is added. This allows quick response when new sensitive data is found or added to monitored systems if it shouldn't be there or is not properly secured.

1.3.4 DatAlert

DatAlert provides real-time alerting for events requiring immediate attention, such as privilege escalations, access to or deletion of sensitive data, permission changes, or changes detected outside of change control hours. Users can define what they want to be alerted about using predefined rulesets and specify how they should be alerted (email, event log, syslog message, Simple Network Management Protocol (SNMP) trap, or trigger a command line script).

1.3.5 Data Transport Engine

Data Transport Engine provides mechanisms for cross-platform migration of data. Users can specify whether to preserve access permissions during migration, or can specify new permissions if the destination requires Access Control List (ACL) modifications. All migrations can be modeled so that users can simulate the migration and determine any issues prior to committing to executing the data transfer.

1.3.6 DatAdvantage UI

DatAdvantage UI is the primary user interface for the TOE. This interface provides the majority of the management and user functionality offered by the TOE, including analysis, reporting, auditing, and modification of monitored system data. This interface is also used to access the DatAlert, IDU Classification Framwork, and Data Transport Engine functionality. DatAdvantage UI is a graphical Windows-based standalone application.

1.3.7 DatAdvantage Management Console

DatAdvantage Management Console is the primary management interface for configuring the TOE and deploying remote components to monitored systems. Administrators also configure general DatAdvantage settings and perform maintenance tasks, such as scheduling and running database jobs, via this interface. DatAdvantage Management Console is a graphical Windows-based standalone application.

1.3.8 PowerShell API

The PowerShell API is a set of Windows PowerShell cmdlets that enable automation of tasks such as deploying remote components, adding functional components to the base DatAdvantage system, and controlling database tasks.

1.4 TOE Diagram

Figure 1 shows the details of the deployment configuration of the TOE[4]. The following are undefined acronyms that appear within the diagram:

- AD – Active Directory
- DB – Database
- SQL – Structured Query Language

[4] Not depicted: all systems make use of the AD server to synchronize time. Connections excluded to aid in readability.

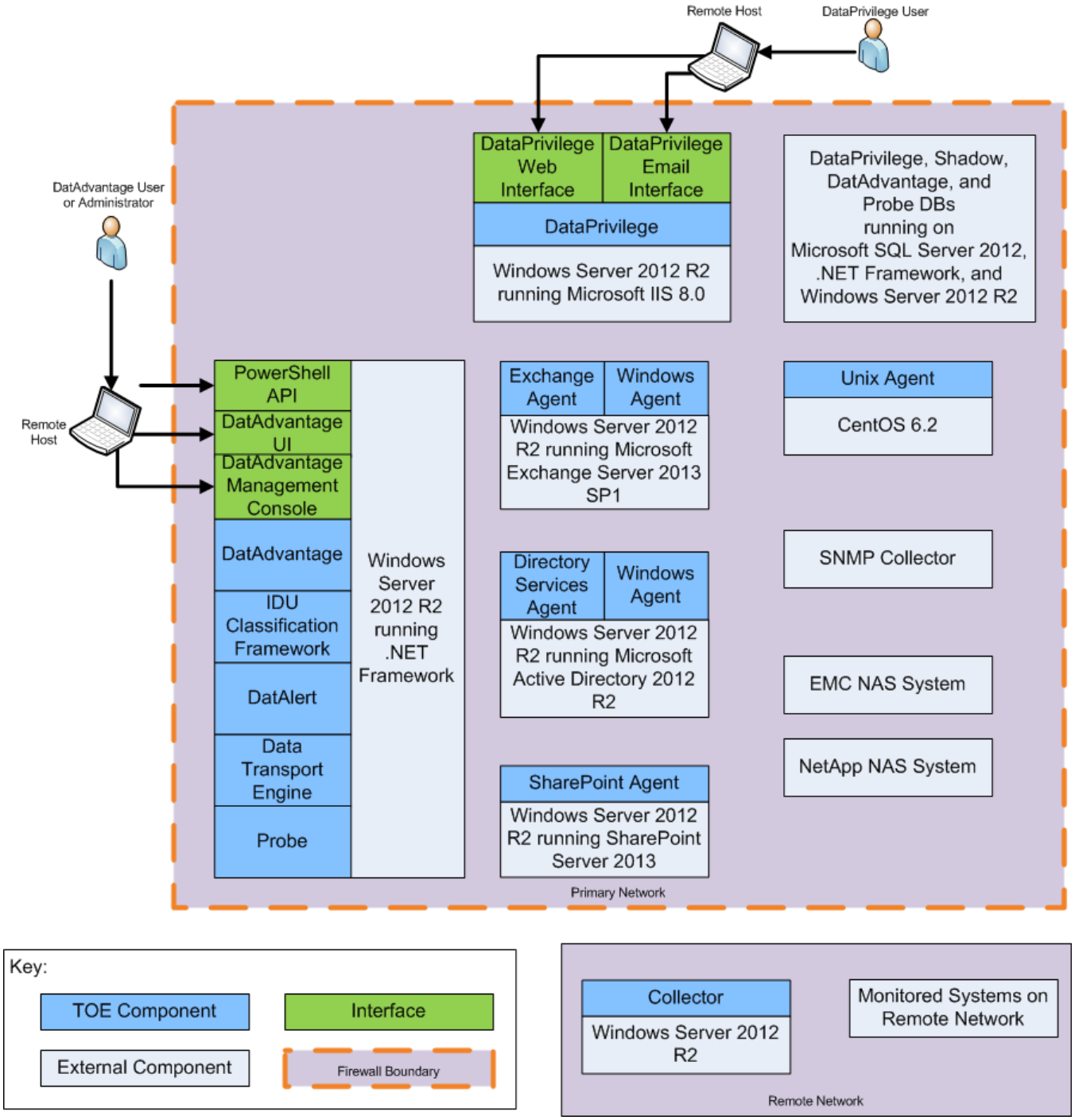

Figure 1 – Deployment Configuration of the TOE

The TOE software is installed from a single binary installer package, in the following configuration:

- DatAdvantage, DatAdvantage UI, DatAdvantage Management Console, PowerShell API, IDU Classification Framework, DatAlert, Data Transport Engine, and probe installed on Windows Server 2012 R2 running .NET Framework
- DataPrivilege installed on Windows Server 2012 R2 running IIS 8.0
- The Collector running on Windows Server 2012 R2

- The Unix Agent running on monitored systems with CentOS
- The Exchange Agent and Windows Agent running on Windows Server 2012 R2 running Exchange Server 2013 SP1
- The Directory Services Agent and Windows Agent running on Windows Server 2012 R2 running Microsoft Active Directory 2012 R2
- The SharePoint Agent running on Windows Server 2012 R2 running SharePoint Server 2013

An AD server provides time synchronization for all of the distributed components and systems present in the evaluated configuration. Probes access EMC and NetApp NAS Systems remotely to gather file and folder access data. DatAdvantage communicates with the AD server to handle user and administrator authentication services. DatAlert communicates with the Simple Mail Transfer Protocol (SMTP) collector and Exchange server in order to send alerts to administrators and users. The Data Transport Engine connects to monitored systems for data migrations, and the probe also connects to these systems (in cases where an agent is not present – as shown by the blue lines in the diagram) to gather object access data. Agents gather data locally and send it to the Probe, which forwards the data to the DatAdvantage component for storage and analysis (as shown in the purple lines in the diagram). Collectors server as a collection point for monitored system data on remote networks and return this data to the probes.

In the evaluated configuration, the TOE is installed in two logically separate network segments protected by a firewall. All of the main components of the TOE are installed in the "Primary Network" as seen in the figure above, while a Collector is installed to manage and capture event data from monitored systems in a "Remote Network". The Primary and Remote networks represent a typicaly deployment of the TOE, e.g. a main office with various file servers and a branch office location with a small handful of file servers or monitored systems. The Collector funnels all data through a secure VPN[5] tunnel back to the probe. In addition, a firewall is used to restrict access to the DataPrivilege interfaces from untrusted users. TOE users are assumed to be on the same logical network as the TOE.

1.4.1 Brief Description of the Components of the TOE

The TOE is delivered to the customer as a single installer package that is used to install the entire Data Governance Suite, which is comprised of the following components:

- DatAdvantage v6.2.38.0 including:
  - PowerShell API v6.2.35.7
  - DatAdvantage Management Console v6.2.35.7
  - DatAdvantage UI v6.2.35.57
  - Probe v6.2.35.7
  - Collector v6.2.35.7
  - Agent software:
    - Exchange Agent v5.9.68.5
    - Windows Agent v6.2.35.57
    - Unix Agent v6.2.181
    - Directory Services Agent v6.2.35.57
- IDU Classification Framework v6.2.35.57
- DataPrivilege v6.0.113 including the DataPrivilege UI

[5] VPN – Virtual Private Network

- DatAlert v6.2.35.57
- Data Transport Engine v6.2.35.57

Once installed, DatAlert and specific platform support (e.g., DatAdvantage for SharePoint, Exchange, Unix/Linux and Directory Services) are activated by license keys entered by the customer via the DatAdvantage Management Console.

The TOE software components are downloaded from the Varonis website as a single binary installer package and installed on a general purpose OS and hardware by the customer. Varonis does not provide the hardware or OS software. Only the TOE software is made available by Varonis to customers.

1.4.2 TOE Environment

The TOE components are installed on OS and hardware as described above in Section 1.4.1. The server components of the TOE are intended to be deployed in a secure data center that protects physical access to the TOE.

The TOE relies on hardware and software that is not part of the TOE for its essential operation. The following non-TOE hardware and software is required for the essential operation of the TOE:

- Microsoft SQL Server 2012 is used to store data collected from monitored systems in the evaluated configuration. The TOE also supports SQL Server 2005, SQL Server 2008, and SQL Server 2014.
- An AD server is necessary in order to synchronize time among all of the distributed components of the TOE and to provide authentication services for the TOE. The version of AD used in the evaluated configuration is Active Directory 2012 R2. The TOE also supports Windows NT[6] 4.0 domain, Windows 2000 Active Directory, Windows 2003 Active Directory, and Windows 2008 Active Directory.
- Server hardware. Table 2 specifies the minimum system requirements for the proper operation of the TOE.
- Windows Server to run the server components of the TOE. The evaluated version of the TOE runs on Windows Server 2012 R2. The TOE also supports Windows 2000, Windows 2003, Windows 2003 R2, Windows 2008, Windows 2008 R2, and Windows 2012.
- An SNMP trap receiver and Microsoft Exchange server to send alerts to notify administrators of specified events via the DatAlert functionality. The TOE supports Microsoft Exchange Server 2013 SP1 in the evaluated configuration.
- All of the monitored systems that the TOE uses to collect data.
- Several components require Microsoft .NET Framework to operate correctly. These include the main server components and the DatAdvantage UI.
- The PowerShell API requires that Windows PowerShell be installed.
- The DataPrivilege Interface requires that Microsoft IIS be installed. The TOE uses IIS 8.0 in the evaluated configuration, but also supports IIS 7.5.
- The TOE uses the Federal Information Processing Standard (FIPS) 140-2 validated cryptographic algorithms provided by the Windows OS in order to provide secure communications.
- A firewall and VPN must be used to protect the network communciations between the Primary and Remote network locations as well as the externally accessible user interfaces.

[6] NT – New Technology

Table 2 Server Minimum System Requirements

Environment Size	CPU[7]	RAM[8]	Disk space
Small or evaluation	2.0 Gigahertz (GHz) or higher	4 Gigabytes (GB) or higher	250 GB
Medium (for the IDU server components)	2.0 GHz or higher x2	8 GB or higher	500 GB
Medium (for the probes)	2.0 GHz or higher x2	8 GB or higher	120 GB
Large or Enterprise (for the IDU server components)	2.0 GHz or higher x4	16 GB or higher	500 GB
Large or Enterprise (for the probes)	2.0 GHz or higher x2	16 GB or higher	120 GB
Large or Enterprise (for the reporting server)	2.0 GHz or higher x4	16 GB or higher	120 GB
Large or Enterprise (for the shadow database)	2.0 GHz or higher x4	16 GB or higher	500 GB

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

The TOE provides other security features that are out of the scope of the TOE. These features are not included in the TOE and will not be evaluated, and therefore there is no assurance level associated with them. The features not included in the TOE are the following:

- DatAnswers and all related management functionality, including DatAnswers PowerShell commands.
- DataPrivilege API, an API for creating third-party permission and membership requests.
- The DrvSet executable included with the installation, a developer interface for troubleshooting the server.

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

The TOE is Data Governance Suite v6.2. The TOE is a distributed system composed of the following elements:

- DatAdvantage, IDU Classification Framework, DatAlert, Data Transport Engine, shadow DB, probe, and collector all installed from a single installation package
- DataPrivilege installed on separate hardware from the same installation package
- DatAdvantage UI installed on separate hardware from the same installation package
- PowerShell API installed on separate hardware from the same installation package
- Windows Agent, Unix Agent, Exchange Agent, SharePoint Agent, Directory Services Agent deployed from the DatAdvantage Management Console

[7] CPU – Central Processing Unit
[8] RAM – Random Access Memory

- The binary installer(s) containing the code to install the TOE software in its entended environment: IDU_Suite_6.2.38.0_GA.zip and IDU_Suite_6.0.113.12_GA.zip (for DataPrivilege only).

Once installed the various features are enabled via license keys entered by the customer. The TOE is installed in its evaluated configuration following the guidance documents listed in Section 1.5.1.1. The TOE installation files are obtained and delivered via the methods described in Section 1.4.1 above.

1.5.1.1 Guidance Documentation

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

- *Metadata Framework 6.2 Installation Guide.pdf*
- *Metadata Framework SQL 2012 Installation Guide.pdf*
- *Metadata Framework 6.2 Installation Prerequisites and Requirements.pdf*
- *Metadata Framework 6.2 PowerShell Reference Guide.pdf*
- *Metadata Framework 6.2 Probe Configuratoin Guide.pdf*
- *Data Transport Engine 6.2 User Guide.pdf*
- *DatAdvantage 6.2 User Guide.pdf*
- *DatAlert 6.2 User Guide.pdf*
- *DataPrivilege 6.0 User Guide.pdf*
- *Management Console 6.2 User Guide.pdf*
- *Metadata Framework 6.2.38 Release Notes.pdf*
- *Metadata Framework 6.0.113 Release Notes.pdf*
- *Configuring DatAdvantage 6.2 for EMC VNX (Celerra) Isilon CEPA Event Collection.pdf*
- *Configuring NetApp Clusters for Metadata Framework 6.2.pdf*

All guidance documentation is available for downloaded from the Varonis support site. No hard copies of documentation are provided.

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 TSF
- Resource Utilization
- Data Collection and Analysis

1.5.2.1 Security Audit

The Security Audit functionality provides the capability to generate logs for security relevant events and records the identity of the subject responsible for initiating the event. Administrators and users can review the logs via the DatAdvantage UI and use its robust selection and ordering functionality to review internal logs. DataPrivilege

Web UI users can also review permission changes they have made. The TOE's internal logs cannot be modified or deleted.

1.5.2.2 User Data Protection

The user Data Protection functionality provides the capability for the Data Transport Engine to migrate data between remote systems. The TOE also permits rollback of pending permission changes prior to or after a commit operation within the DatAdvantage UI. The TOE enforces an access control policy to ensure that only users and administrators that have been assigned a sufficient role can access this functionality.

1.5.2.3 Identification and Authentication

The Identification and Authentication functionality requires users and administrators to identify and authenticate before gaining access to any TOE functionality. Authentication is via a remote trusted AD server. The TOE maintains the AD identifier and the role for each account.

1.5.2.4 Security Management

The Security Management functionality provides the capability for administrators and users with appropriate roles to manage the security functionality, data, and attributes provided by the TOE. This functionality also describes the roles available to manage the TOE.

1.5.2.5 Protection of the TSF

The Protection of the TSF functionality ensures that ACL data is maintained during Data Transport Engine migrations.

1.5.2.6 Resource Utilization

The Resource Utilization functionality enforces maximum CPU utilization quotas for agents.

1.5.2.7 Data Collection and Analysis

The Data Collection and Analysis functionality provides the capability for the TOE to gather data from remote systems. The TOE also performs analysis of the data to discover potential security violations. Data gathered from remote systems is stored such that it cannot be modified or deleted and can be archived for extended storage. If a security violation is detected then the TOE can use custom alerts to notify users and administrators.

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 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the Common Evaluation Methodology (CEM) as of 2016-09-27 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented with Flaw Remediation (ALC_FLR.2)

3. Security Problem

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

- Known and presumed threats countered by either the TOE or by the security environment
- OSPs 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 assets against which protection is required by the TOE or by the security environment. The threat agents are divided into three categories:

- Attacker who is not a TOE user: entities or processes that have public knowledge of how the TOE operates and is assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters, and no physical access to the TOE.
- TOE user: user with no administrative rights (or processes belonging to such users) that have extensive knowledge of how to use the TOE, is assumed to possess a moderate skill level, no access to alter TOE configuration settings or parameters, and physical access to the TOE.

Each are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[9] 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. Table 4 below lists the applicable threats.

Table 4 – Threats

Name	Description
T.AUDACC	Persons may not be accountable for the actions that they conduct because security relevant actions may not be recorded or viewable, thus allowing an "attacker who is not a TOE user" to escape detection.
T.AVOID_DETECTION	An "attacker who is not a TOE user" may attempt to temporarily disable connectivity between physically separate components of the TOE in order to prevent detection of a potential security breach.
T.BADSTATE	An "attacker who is not a TOE user" may exploit protocol vulnerabilities or misconfigurations in monitored IT entities that are configured in an insecure state without any TOE users being notified.
T.EXPLOIT	An "attacker who is not a TOE user" may tamper with the remote components of the TOE such that the systems reach a vulnerable state due to overuse of resources.
T.MASQUERADE	A "TOE user" may masquerade as another entity in order to gain unauthorized access to data or TOE resources.

[9] TSF – TOE Security Functionality

Name	Description
T.MIGRATION	When migrating files and folders between different systems on the network, a “TOE user” may lose or misconfigure ACL data for the new environment, resulting in an insecure configuration.
T.NETWORK_FAILURE	The systems hosting the TOE or the network to which the TOE is connected may fail, causing a disruption in network connectvitiy between TOE server components and remote collectors, probes, and agents.
T.TSF_COMPROMISE	An “attacker who is not a TOE user” may be able to access TOE functionality without an appropriate role.

3.2 Organizational Security Policies

There are no OSPs defined for this evaluation.

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.ADMIN_PROTECT	No malicious software is installed or running on the remote hosts accessing the TOE and the TOE environment, or on the machines hosting the TOE and TOE environment.
A.DOMAIN	All TOE users are identified and authenticated by the IT environment within the same domain as the TOE.
A.FIPS	FIPS 140-2 validated cryptographic algorithms in the TOE environment must provide all secure communications for the TOE.
A.FIREWALL	All ports needed for proper operation of the TOE will be opened at the firewall. Also, any firewall settings necessary for the TOE's operation will be configured to allow the TOE to operate. In addition, a VPN tunnel will be used to protect the communciations between the Primary Network and the Remote Network.
A.INSTALL	The TOE is installed on a server platform running an operating system dedicated to the TOE and its server components.
A.LOCATE	The TOE, monitored systems, switches, monitored networks, firewall, and NTP, SMTP, and LDAP servers are located within a controlled access facility. All of the above components are installed in a Primary Network while the TOE Collector software and any combination of monitored systems may be installed in the Remote Network. Both locations share the same physical protections and access restrictions.
A.EMAIL	The email accounts used by the TOE to send notifications are associated with accounts in a domain for which the TOE is also a member. Emails are not sent by the TOE to an

Name	Description
	external SMTP server, and the email server used by the TOE does not accept direct communication from external SMTP servers. Any clients, including the TOE, and those accessing the SMTP server from outside of the controlled access facility, do so using TLS.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NETCON	The TOE environment provides the network connectivity required to allow the TOE to provide secure access control monitoring functions.
A.NOEVIL	The administrators of the TOE are non-hostile, appropriately trained, and follow all guidance. Administrators will never accept unknown or untrusted certificates for the web or email communication with the TOE.
A.OS_ACCESS	The TOE environment is in a secure state and provides a sufficient level of protection to itself and the TOE components.
A.SECCOMM	The environment provides a sufficient level of protection to secure communications between distributed TOE components and the TOE server components.
A.TIMESTAMP	The TOE environment provides the TOE with the necessary reliable timestamps.

4. Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition. 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.AUTHENTICATE	The TOE must identify and authenticate users before allowing access to any TOE functionality.
O.BACKGROUND_PROCESS	The TOE must be able to collect event data without causing undue strain or overuse of the CPU on systems where data collection takes place.
O.DATA_TRANSFER	The TOE must allow authorized users and administrators to move data across the systems on the network.
O.LOG	The TOE must record events of security relevance, provide authorized users and administrators with the ability to review the recorded events, and prevent unauthorized modification or deletion of recorded events.
O.MANAGE	The TOE must provide it's functionality only to authorized users and administrators in order to limit access to the security-relevant functionality of the TOE.
O.MONITOR	The TOE must be able to monitor machines on the network to ensure that they exist in a secure state and alert TOE users if a system enters an insecure state.

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.ADMIN_PROTECT	The administrative and user workstations, as well as the machines hosting the TOE and its environment must be protected from any external interference or tampering.
OE.CONNECT	The TOE environment must be implemented such that the TOE is appropriately located within and connected to the network to perform its intended function.
OE.FIPS	The operating system that the TOE is installed on must provide FIPS 140-2 validated cryptographic algorithms for the TOE to use to establish secure connections.
OE.FIREWALL	Any firewalls in the TOE environment must be configured such that all ports needed for the proper operation of the TOE are open and restricted from access from untrusted users. In addition, a VPN tunnel must be configured to protect the communciations between the Primary and the Remote Network.
OE.OS_ACCESS	The operating system upon which the TOE is installed provides a sufficient level of protection for itself and the TOE software it contains.
OE.PLATFORM	The TOE environment must contain the hardware and operating system upon which the TOE is installed.
OE.SECCOMM	The TOE environment must provide mechanisms to secure communications among TOE agents, probes, collectors, and the server components of the TOE.
OE.TIME	The TOE environment must provide reliable timestamps for the TOE.

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
NOE.MANAGE	Sites depoying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all guidance.
NOE.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.

5. Extended Components

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

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 9 identifies all extended SFRs implemented by the TOE.

Table 9 – Extended TOE Security Functional Requirements

Name	Description
FDC_ANA.1	System Analysis
FDC_SCN.1	System Scan
FDC_STG.1	Scanned Data Storage

5.1.1 Class FDC: Data Collection and Analysis

Data Collection and Analysis functions involve:

- Monitoring systems to obtain data,
- Storing the collected data,
- Performing analysis on collected data and presenting analytical results to administrators in a format that allows them to take appropriate actions

The FDC: Data Collection and Analysis class was modeled after the CC FAU: Security Audit class. The extended family and related components for FDC_ANA: System Analysis were modeled after the CC family and related components for FAU_SAA: Security Audit Analysis. The extended family FDC_SCN: System Scan was modeled after the CC family FAU_GEN: Security Audit Data Generation. The extended family FDC_STG: Scanned Data Storage was modeled after the CC family FAU_STG: Security Audit Event Storage.

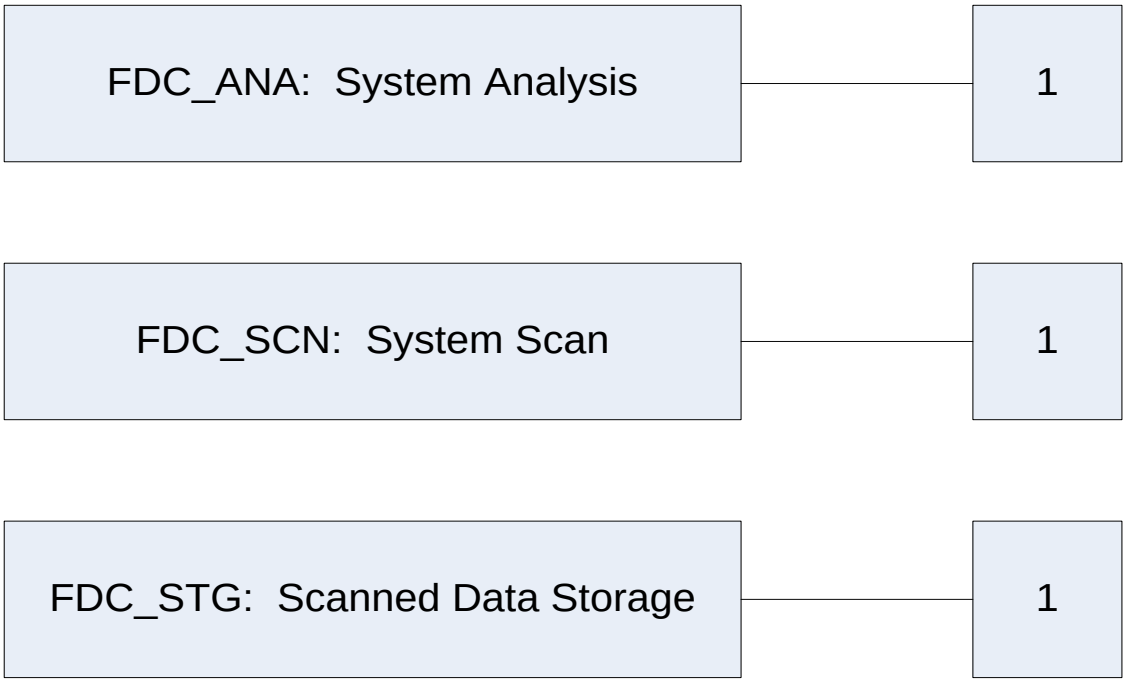

Figure 2 – FDC: Data Collection and Analysis Class Decomposition

5.1.1.1 FDC_ANA: System Analysis

Family Behavior

This family defines the requirements for the use of tools for the analysis of collected data and that allow administrators to react to potential security violations found during analysis of collected data.

Component Leveling

Figure 3 – FDC_ANA: System Analysis family decomposition

FDC_ANA.1 : System Analysis provides the capability to analyze collected data and present the results to administrators in a way that easily allows the administrators to respond to potential security violations found during the analysis.

Management: FDC_ANA.1
The following actions could be considered for the management functions in FMT:

- Maintenance (deletion, modification, addition) of the analysis rules or the set of systems the rules are applied to.

Audit: FDC_ANA.1 System Analysis
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Identity of the entity who initiated a scan or permission change.
- Minimal: Identity of the scanned machines, list of subjects discovered, list of permissions available to each subject.

FDC_ANA.1 System Analysis

Hierarchical to: **No other components.**

FDC_ANA.1.1

The TSF shall be able to apply a set of rules in analyzing collected permission data and based upon these rules indicate potential security violations:

a) Activity monitoring and computer learning to determine subject access to files and folders,
b) Regular expression analysis to determine which files and folders containing sensitive data are at risk for security violations and the subjects that have access to and have accessed sensitive data.

FDC_ANA.1.2

The TSF shall enforce the following set of rules for monitoring scanned data:
Accumulation or combination of [assignment: *subset of defined collected data*] known to indicate a potential security violation;
[assignment: *any other rules*].

FDC_ANA.1.3

The TSF shall be able to indicate a possible security violation to [assignment: *list of users with permission to review analytical results*] and allow [assignment: *list of users with permission to modify user and file security configurations*] to address security violations that are discovered.

Dependencies: **FDC_SCN.1.**

5.1.1.2 FDC_SCN: System Scan

Family Behavior

This family defines the requirements for monitoring systems to collect data about subject and file system permissions and access behaviors.

Component Leveling

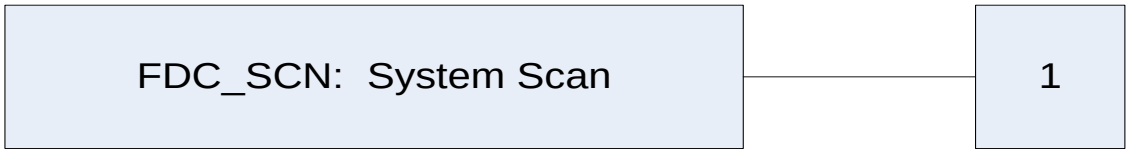

Figure 4 – FDC_SCN: System Scan family decomposition

FDC_SCN.1 System Scan defines the monitoring function and specifies which machines will be monitored.

Management: FDC_SCN.1

- There are no management activities foreseen.

Audit: FDC_SCN.1

- There are no auditable events foreseen.

FDC_SCN.1 System Scan

Hierarchical to: No other components.

FDC_SCN.1.1

The system shall be able to monitor and collect the following information from the targeted IT system resource(s):

a) Permission data for files, folders, mailboxes, directory services, and SharePoint Sites and lists.
b) A log of successful file access attempts for all systems and failed access attempts for Windows file servers and EMC Celerra devises accessed via NFS by subjects on the monitored systems.
c) Detection of sensitive data within files and folders on CIFS/NTFS-capable and SharePoint monitored systems.

FDC_SCN.1.2

The TSF shall record within activity logs at least the following information:

- Date and time of the access, name of the file or folder accessed, path of the file or folder accessed, name of the subject initiating the access, and the operation performed as a result of the access.

FDC_SCN.1.3

The TSF shall record within scans for classified data at least the following information:

- Classification of the type of sensitive data, location of the sensitive data, and the date and time the access occurred.

Dependencies: None.

5.1.1.3 FDC_STG: Scanned Data Storage

Family Behavior

This family defines the requirements for protecting stored scan data.

Component Leveling

Figure 5 – FDC_STG: Scanned Data Storage family decomposition

FDC_STG.1 Scanned Data Storage defines how the TSF protects stored monitor data from unauthorized modification or deletion.

Management: FDC_STG.1

- There are no management activities foreseen.

Audit: FDC_STG.1

- There are no auditable events foreseen.

FDC_STG.1 Scanned Data Storage

Hierarchical to: **No other components.**

FDC_STG.1.1

The TSF shall protect the stored collected data from unauthorized deletion.

FDC_STG.1.2

The TSF shall be able to prevent unauthorized modifications to the stored collected data.

FDC_STG.1.3

The TSF shall allow archival of the stored collected data to authorized users and administrators with the role [assignment: *roles authorized to archive stored collected data*] for an administrator- or user-configured time period.

FDC_STG.1.4

The TSF shall indicate a failure to properly store collected data by performing the following actions: [assignment: *list of actions that are used to notify administrators of a storage failure*].

Dependencies: **FDC_SCN.1.**

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this ST.

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 and italicized text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- 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 10 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 10 – TOE Security Functional Requirements

Name	*Description*	*S*	*A*	*R*	*I*
FAU_GEN.1	*Audit Data Generation*	✓	✓	✓	
FAU_GEN.2	*User Identity Association*				
FAU_SAR.1	*Audit review*		✓		
FAU_SAR.3	*Selectable audit review*		✓		
FAU_STG.1	*Protected audit trail storage*	✓			
FDP_ACC.1	*Subset access control*		✓		
FDP_ACF.1	*Security attribute based access control*		✓		
FDP_ETC.1	*Export of user data without security attributes*		✓		
FDP_ITC.1	*Import of user data without security attributes*		✓		
FDP_ROL.1	*Basic rollback*		✓		

Name	*Description*	*S*	*A*	*R*	*I*
FIA_ATD.1	*User attribute definition*		✓		
FIA_UAU.2	*User authentication before any action*				
FIA_UID.2	*User identification before any action*				
FMT_MOF.1	*Management of security functions behaviour*	✓	✓		
FMT_MSA.1	*Management of security attributes*	✓	✓		
FMT_MSA.3	*Static attribute initialisation*	✓	✓		
FMT_MTD.1	*Management of TSF data*	✓	✓		
FMT_SMF.1	*Specification of management functions*		✓		
FMT_SMR.1	*Security roles*		✓		
FPT_TDC.1	*Inter-TSF basic TSF data consistency*		✓		
FRU_RSA.1	*Maximum quotas*	✓	✓		
FDC_ANA.1	*System Analysis*		✓		
FDC_SCN.1	*System Scan*				
FDC_STG.1	*Scanned Data Storage*		✓		

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

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~~ TOE services;
b. All auditable events, for the [*not specified*] level of audit; and
c. [
   - DatAdvantage: *user and administrator login and logout, file permission changes, account management operations, and file migrations*
   - *DataPrivilege: actions on permission requests*].

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 startup and shutdown of the audit function is implicit through the startup and shutdown of the services that comprise the TOE. The startup and shutdown events can be displayed through the Windows Event Viewer.

FAU_GEN.2 User identity association

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

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 [*all authenticated users and administrators*] 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_SAR.3 Selectable audit review

Hierarchical to: No other components.
Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1

The TSF shall provide the ability to apply [*selection based on:*

- *when the event occurred*
- *which system the event occurred in*
- *which subject generated the event*
- *which object was accessed*
- *which files were accessed*
- *which user received the email*
- *which user sent the email*
- *which file was attached*

And ordering based on:

- *Affected Share Path*
- *Changed Permission (Windows Only)*
- *Changed Permission Flags (Windows Only)*
- *Event Count*
- *Event Description*
- *Event Identifier (ID)*
- *Event Operation*
- *Event Status*
- *Event Type,*
- *File Server / Domain*
- *File Type*
- *Inherited Permission Change*
- *IP / Hostname*
- *Last Occurrence*
- *Number of Nested Files in Deleted Folder*

- *Object*
- *Object Type*
- *Operation By*
- *Operation Source*
- *Path*
- *Permissions After Change (Windows Only)*
- *Permissions Before Change (Windows Only)*
- *Size of Deleted Folder (in Megabytes (MB))*
- *Time*
- *Trustee (Windows Only)*
- *Trustee Account Type (Windows Only)*
- *Account Management*
- *AD Properties*
- *Classification*
- *Follow Up*
- *Filesystem (FS) Properties*
- *Mail Properties*

]

on audit data based on [*no additional criteria*].

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1

The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2

The TSF shall be able to [*prevent*] unauthorized modifications to the stored audit records in the audit trail.

6.2.2 Class FDP: User Data Protection

FDP_ACC.1 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 [*TOE User and Administrator Access Control SFP*] on [

Subjects:

- TOE user and administrator accounts

Objects:

- ACL data collected from files, folders, SharePoint sites and lists, Exchange mailboxes, and Active Directory domains on monitored systems

Operations:

- View, modify, rollback changes, import, export

].

FDP_ACF.1 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 [*TOE User and Administrator Access Control SFP*] to objects based on the following: [

Subject attributes:

- Account Identifier
- Role

Object attributes:

- ACL entries

].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*if the user or administrator's account identifier is associated with a role that can perform an operation, the operation is allowed. Otherwise, the operation is denied*].

FDP_ACF.1.3

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

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [*"ownership", e.g., optionally, access can be denied to all users who are not "owners" as configured by an administrator*].

FDP_ETC.1 Export of user data without security attributes

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FDP_ETC.1.1

The TSF shall enforce the [*TOE User and Administrator Access Control SFP*] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2

The TSF shall export the user data without the user data's associated security attributes.

FDP_ITC.1 Import of user data without security attributes

Hierarchical to: No other components.

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

FDP_ITC.1.1

The TSF shall enforce the [*TOE User and Administrator 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: [*only users with the Enterprise Manager or Power User role may execute an import task*].

FDP_ROL.1 Basic rollback

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FDP_ROL.1.1

The TSF shall enforce [*TOE User and Administrator Access Control SFP*] to permit the rollback of the [*modification of ACL entries*] on the [*files, folders, Exchange mailboxes, Active Directory domains, and SharePoint shares and lists on monitored systems*].

FDP_ROL.1.2

The TSF shall permit operations to be rolled back within the [*prior to being committed by an Enterprise Manager or Power User, after being committed by an Enterprise Manager or Power User*].

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: [*Active Directory account identifier associated with the user's account, role*].

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.

6.2.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

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

FMT_MOF.1.1

The TSF shall restrict the ability to [*determine the behavior of, enable, modify the behavior of*] the functions [*Data Transport Engine data transfer, email alerts, deployment of agents, probes, and collectors*] to [*the Enterprise Manager, System Administrator, and Power User roles*].

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1

The TSF shall enforce the [*TOE User and Administrator Access Control SFP*] to restrict the ability to [modify] the security attributes [*TOE user or administrator account permissions*] to [*the Enterprise Manager and System Administrator roles*].

FMT_MSA.3 Static attribute initialization

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 [*TOE User and Administrator Access Control SFP*] to provide [*[restrictive]*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*no roles*] to specify alternative initial values to override the default values when an object or information is created.

Application note: the default permissions for new accounts are "User" role permissions, which can view most data, but cannot modify data.

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 [modify, delete, *[create, commit]*] the [*ACL changes for monitored systems*] to [*the Enterprise Manager and Power User roles*].

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: [

- *Management of TOE user and administrator accounts*
- *Management of ACL changes for files, folders, mailboxes, shares, and directories on monitored systems*
- *Management of Data Transport Engine data transfers*
- *Management of the alerting capabilities of the TOE*
- *Management of agents, probes, and collectors*

].

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 [

- *DatAdvantage: Enterprise Manager, Power User, System Administrator, and User*
- *DataPriviledge: Administrator, Data Owner, Group Owner, Authorizer, Floor Support, and User*

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Application note: Within documentation references, unless otherwise noted, DatAdvantage "administrators" are any accounts with the roles "Enterprise Manager" or "System Administrator", whereas "users" are any accounts with the roles"Power User" and "User".

6.2.5 Class FPT: Protection of the TSF

FPT_TDC.1 Inter-TSF basic TSF data consistency

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_TDC.1.1

The TSF shall provide the capability to consistently interpret [*ACL data*] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2

The TSF shall use [*an administrator-defined set of rules mapping ACL data from source object to destination object*] when interpreting the TSF data from another trusted IT product.

6.2.6 Class FRU: Resource Utilization

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: [*agent CPU utilization*] that [*subjects*] can use [*simultaneously*].

6.2.7 Class FDC: Data Collection and Analysis

FDC_ANA.1 System Analysis

Hierarchical to: **No other components.**

Dependencies: **FDC_SCN.1.**

FDC_ANA.1.1

The TSF shall be able to apply a set of rules in analyzing collected permission data and based upon these rules indicate potential security violations:

a) Activity monitoring and computer learning to determine subject access to files and folders,

b) Regular expression analysis to determine which files and folders containing sensitive data are at risk for security violations and the subjects that have access to and have accessed sensitive data.

FDC_ANA.1.2

The TSF shall enforce the following set of rules for monitoring scanned data:

- Accumulation or combination of [*ACL data on objects and the end users that can access those objects, users access behavior to objects containing sensitive data*] known to indicate a potential security violation;
- [*no additional rules*].

FDC_ANA.1.3

The TSF shall be able to indicate a possible security violation to [*users with the Power User or User roles*] and allow [*users with the Power User role*] to address security violations that are discovered.

Application note: "sensitive data" includes data that matches patterns and regular expressions defined by an administrator or user.

FDC_SCN.1 System Scan

Hierarchical to: **No other components.**

Dependencies: **None.**

FDC_SCN.1.1

The system shall be able to monitor and collect the following information from the targeted IT system resource(s):

a) Permission data for files, folders, mailboxes, Active Directories, and Sharepoint sites and lists.

b) A log of successful file access attempts for all systems and failed access attempts for Windows file servesr and EMC Celerra devices access via NFS by subjects on the monitored systems.

c) Detection of sensitive data within files and folders on CIFS/NTFS-capable and SharePoint monitored systems.

FDC_SCN.1.2

The TSF shall record within activity logs at least the following information:

- Date and time of the access, name of the file or folder accessed, path of the file or folder accessed, name of the subject initiating the access, and the operation performed as a result of the access.

FDC_SCN.1.3

The TSF shall record within scans for classified data at least the following information:

- Classification of the type of sensitive data, location of the sensitive data, and the date and time the access occurred.

FDC_STG.1 Scanned Data Storage

Hierarchical to: **No other components.**

Dependencies: **FDC_SCN.1.**

FDC_STG.1.1

The TSF shall protect the stored collected data from unauthorized deletion.

FDC_STG.1.2

The TSF shall be able to prevent unauthorized modifications to the stored collected data.

FDC_STG.1.3

The TSF shall allow archival of the stored collected data to authorized users and administrators with the role [*Enterprise Manager*] for an administrator- or user-configured time period.

FDC_STG.1.4

The TSF shall indicate a failure to properly store collected data by performing the following actions: [*sending an email alert to a specified list of email addresses*].

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 11 summarizes these requirements.

Table 11 – 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[10] system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

[10] CM – Configuration Management

7. TOE Summary Specification

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

7.1 TOE Security 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 12 lists the security functionality and their associated SFRs.

Table 12 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_ETC.1	Export of user data without security attributes
	FDP_ITC.1	Import of user data without security attributes
	FDP_ROL.1	Basic rollback
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_MOF.1	Management of security functions behaviour
	FMT_MSA.1	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

TOE Security Functionality	SFR ID	Description
Protection of TOE Security Functions	FPT_TDC.1	Inter-TSF basic TSF data consistency
Resource Utilization	FRU_RSA.1	Maximum quotas
Data Collection and Analysis	FDC_ANA.1	System Analysis
	FDC_SCN.1	System Scan
	FDC_STG.1	Scanned Data Storage

7.1.1 Security Audit

DatAdvantage generates internal logs for user and administrator login and logout, file permission changes, account management operations, and file migrations.

DataPrivilege audits actions on permission requestspermission changes. These interfaces represent the full set of user and administrator interfaces used to interact with the TOE and the functionality it provides. All audit records include the user account name of the subject initiating the event.

Within the internal audit records, the TOE records the following information:

Table 13 – Audit Record Contents

Field	Content
Time	Date and time that the event occurred.
Operation Type	The type of operation that was performed.
Operation By	Identity (user account name) of the subject initiating the operation.
Event Status	Indicates whether the event was successful or not.
Event Description	Provides additional details about the log event to aid in administrator understanding of the event.

All users and administrators have access to view the logs via the DatAdvantage UI. This interface also provides a powerful suite of features that can be used to sort and order the audit records by a variety of criteria, as enumerated above in FAU_SAR.3. This includes only showing the audit records based on certain selection criteria, and then ordering the visible records based on a number of different ordering criteria. All audit records are stored for an administrator-determined time period and cannot be deleted manually from any of the interfaces provided by the TOE. In addition to the DatAdvantage UI, the DataPrivilege Web UI provides the ability to review permission changes that a user has made.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.3, FAU_STG.1.

7.1.2 User Data Protection

The DatAdvantage UI provides data transfer and rollback functionality to users and administrators with the Enterprise Manager and Power User roles. The data transfer functionality allows users and administrators to transfer data from one monitored system to another via the DatAdvantage UI. Data transferred via this method can retain the access controls associated with the files and folders that are transferred. This allows the security configurations to be maintained while data is transferred to different systems around the network.

The rollback functionality allows users and administrators to revert changes made by users without a sufficient role to commit changes. All changes are queued for implementation until a commit command is issued, which results in all or a subset of pending changes being implemented. Once a commit has been issued, most of these changes can still be reverted, except any files or folders that have been migrated as a result of the commit.

The TOE controls access to functionality that enabled viewing, modification, or rollback of changes to user data via a standard access control policy. The TOE User and Administrator Access Control SFP permits access to functionality if the user or administrator has a role that permits access to the functionality.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_ETC.1, FDP_ITC.1, FDP_ROL.1.

7.1.3 Identification and Authentication

The TOE uses a remote trusted Active Directory server to authenticate credentials passed by users. The results of authentication are returned, either a success or failure message for Lightweight Directory Access Protocol (LDAP). Prior to authenticating, users and administrators are not given access to any TOE functionality. Users must pass valid credentials to the TOE for authentication to be successful. The TOE stores and maintains each user's and administrator's role and a mapping to the user's Active Directory username.

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

7.1.4 Security Management

The TOE provides methods to manage the security functionality, TSF data, and security attributes. The security functionality includes Data Transport Engine data transfers that can be used to transfer data relevant to user accounts or directories used for TOE authentication. Email alerts can be set up for various security-related notifications, including when a monitored system loses connectivity with the TOE. Administrators can manage the deployment of agents, probes, and collectors to monitored systems across the network. Administrators can manage account permissions for TOE user and administrator accounts. Users with sufficient permissions can create, delete, modify, and commit changes to ACL data on monitored systems.

Management activities and most of the primary TOE user functionality takes place via the DatAdvantage UI and the Management Console. The TOE also provides an API (a set of Windows PowerShell cmdlets) that can be used for maintenance tasks and automating the deployment of agents, probes, and collectors. The other interfaces provided by the TOE do not provide access to management functionality, but can be used to work with user data.

DatAdvantage uses four primary roles to control access to management and user functionality. The Enterprise Manager role has full access to all user and management functionality provided by the TOE. The System

Administrator role has access to manage the TOE configuration, but cannot commit changes to user data. The Power User role has no access to the TOE configuration, but can commit changes to user data. The User role can only view collected data and reports and make changes to user data, but not commit them.

DataPrivilege also has a set of roles used to provide fine-grained control over access to various functions in DataPrivilege. These include Administrators, which are responsible for managing ownership and various configuration settings, Data Owners, which are responsible for managing folder access, Group Owners, which are responsible for managing groups, Authorizers, which are responsible for handling permission requests, Floor Support, which can view pending requests, and Users, who can submit permission requests.

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

7.1.5 Protection of the TSF

When transferring files and folders to other monitored systems via the Data Transport Engine functionality provided by the TOE, the ACL data tied to these objects is maintained by the TOE. The TOE allows users and administrators to define the criteria for which source machine the data is copied from, the actual files and folders to be copied, which permissions, folder structures, and file attributes to copy, which destination machine the data is copied to, and how to handle collisions if they occur during the transfer operation.

TOE Security Functional Requirements Satisfied: FPT_TDC.1.

7.1.6 Resource Utilization

The TOE enforces maximum CPU utilization of 10% for agents operating on monitored systems. The agent will automatically terminate any running tasks if this limit is exceeded. Agents also terminate any running tasks if total CPU utilization on the system exceeds 95%. The TOE reads the CPU utilization every ten seconds, and must receive six consecutive overutilization readings before the agent is terminated.

TOE Security Functional Requirements Satisfied: FRU_RSA.1.

7.1.7 Data Collection and Analysis

This class describes the primary user functionality provided by the TOE. The TOE gathers permission data on files, folders, mailboxes, shares, and directories, records all successful file access attempts, all failed access attempts for Windows file servers and NFS access to EMC Celerra devices, and scans files on Windows file servesr, CIFS/NTFS-compatable NAS devices, and SharePoint sites for sensitive data (such as credit card information, social security numbers, etc.). The TOE uses agents, probes, and collectors in order to gather this information. Probes are small programs that are installed in close proximity to monitored systems and gather data from across the network. Agents are processes that run directly on the monitored system and perform local data collection to gather the log and file data recorded by the TOE. The TOE can also optionally deploy Collectors, which are small services that sit between monitored systems and Probes. Collectors are often used when the monitored system exists on a separate network. The TOE sends an email alert to a list of specified user and administrator email addresses in the event that a probe, collector, or agent fails to return any collected event data to the TOE.

The TOE records a variety of information about the access, including the information enumerated in FDC_SCN.1.1. The TOE also scans for sensitive information (such as credit card information, social security numbers, etc.) within the files, as opposed to just scanning for file access data and permission data. The TOE determines where potentially insecure access to sensitive data is present.

Once collected, the information from monitored systems is stored within a database controlled by the TOE. Since none of the interfaces provided by the TOE grant direct access to the database, no user or administrator can modify or delete the collected information. The DatAdvantage Management Console allows configuration of automatic archiving and archiving after a specific time period.

The TOE applies activity montoring and computer learning to detect patterns of access to data that represent a potential security breach. All files are monitored and suspicious patterns of access are identified as the TOE monitors the users who typically access those files and their usage patterns. The TOE also identifies files and folders containing sensitive data that might be accessible to users who do not need to access the data. This represents a potential breach of security and is recommended for remediation. Users and administrators can define custom alerts to notify them of potential security violations. The alerts can be sent via syslog, internal logs, SNMP traps, SMTP email messages, or configured to execute a command line script.

TOE Security Functional Requirements Satisfied: FDC_ANA.1 , FDC_SCN.1 , FDC_STG.1 .

8. Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 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 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

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

Table 14 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.AUDACC Persons may not be accountable for the actions that they conduct because security relevant actions may not be recorded or viewable, thus allowing an “attacker who is not a TOE user” to escape detection.	O.LOG The TOE must record events of security relevance, provide authorized users and administrators with the ability to review the recorded events, and prevent unauthorized modification or deletion of recorded events.	O.LOG couners this threat by ensuring that an audit trail of security-relevant events on the TOE is preserved.
	OE.TIME The TOE environment must provide reliable timestamps for the .	OE.TIME counters this threat by ensuring that accurate timestamps are provided for all audit records, allowing the order of events to be preserved.
T.AVOID_DETECTION An “attacker who is not a TOE user” may attempt to temporarily disable connectivity between physically separate components of the TOE in order to prevent detection of a potential security breach.	OE.ADMIN_PROTECT The administrative and user workstations, as well as the machines hosting the TOE and its environment must be protected from any external interference or tampering.	OE.ADMIN_PROTECT counters this threat by ensuring that non-TOE users cannot tamper with the TOE or its environment.
	NOE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	NOE.PHYSICAL counters this threat by ensuring that unauthorized users are prevented from gaining physical access to the TOE or its environment.
T.NETWORK_FAILURE The systems hosting the TOE or the network to which the TOE is connected may fail, causing a disruption in network connectvitiy	OE.CONNECT The TOE environment must be implemented such that the TOE is appropriately located within and connected	OE.CONNECT counters this threat by ensuring that the TOE environment provides a reliable network connection necessary to support data collection by the TOE.

Threats	Objectives	Rationale
between TOE server components and remote collectors, probes, and agents.	to the network to perform its intended function.	
T.BADSTATE An “attacker who is not a TOE user” may exploit protocol vulnerabilities or misconfigurations in monitored IT entities that are configured in an insecure state without any TOE users being notified.	O.MONITOR The TOE must be able to monitor machines on the network to ensure that they exist in a secure state and alert TOE users if a system enters an insecure state.	O.MONITOR counters this threat by ensuring that systems on the network are monitored by the TOE and that the TOE alerts its users and administrators when a security violation occurs.
	NOE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	NOE.PHYSICAL mitigates part of this threat because the TOE resides in a controlled access facility.
T.EXPLOIT An “attacker who is not a TOE user” may tamper with the remote components of the TOE such that the systems reach a vulnerable state due to overuse of resources.	O.BACKGROUND_PROCESS The TOE must be able to collect event data without causing undue strain or overuse of the CPU on systems where data collection takes place.	O.BACKGROUND_PROCESS counters this threat by ensuring that the remote components of the TOE do not exceed a quota on how much CPU they can utilize at any given time.
	NOE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	NOE.PHYSICAL mitigates part of this threat because the TOE resides in a controlled access facility.
T.MASQUERADE A “TOE user” may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.AUTHENTICATE The TOE must identify and authenticate users before allowing access to any TOE functionality.	O.AUTHENTICATE counters this threat by ensuring that the TOE is able to store login information about users and use it to identify and authenticate users before granting access to any TOE functionality.
T.MIGRATION When migrating files and folders between different systems on the network, a “TOE user” may lose or misconfigure ACL data for the new environment, resulting in an insecure configuration.	O.DATA_TRANSFER The TOE must allow authorized users and administrators to move data across the systems on the network.	O.DATA_TRANSFER counters this threat by ensuring that TOE users and administrators can transfer data across the network while maintaining a secure state for the resulting deployment.
T.TSF_COMPROMISE An “attacker who is not a TOE user” may be able to access TOE functionality without an appropriate role.	NOE.MANAGE Sites depoying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all guidance.	NOE.MANAGE counters this threat by ensuring all TOE administrators are appropriately trained and competent to configure the TOE and keep it in a secure state.
	O.MANAGE The TOE must provide it's functionality only to authorized users and administrators in order to limit access to the security-relevant functionality of the TOE.	O.MANAGE counters this threat by restricting the management functions of the TOE to authorized users.

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 OSPs defined for this evaluation.

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.ADMIN_PROTECT No malicious software is installed or running on the remote hosts accessing the TOE and the TOE environment, or on the machines hosting the TOE and TOE environment.	OE.ADMIN_PROTECT The administrative and user workstations, as well as the machines hosting the TOE and its environment must be protected from any external interference or tampering.	OE.ADMIN_PROTECT upholds this assumption by ensuring that the systems in the TOE and the TOE environment are protected from external interference and tampering.
A.DOMAIN All TOE users are identified and authenticated by the IT environment within the same domain as the TOE.	OE.CONNECT The TOE environment must be implemented such that the TOE is appropriately located within and connected to the network to perform its intended function.	OE.CONNECT upholds this assumption by ensuring that the TOE has been located within the proper domain.
A.FIPS FIPS 140-2 validated cryptographic algorithms in the TOE environment must provide all secure communications for the TOE.	OE.FIPS The operating system that the TOE is installed on must provide FIPS 140-2 validated cryptographic algorithms for the TOE to use to establish secure connections.	OE.FIPS upholds this assumption by ensuring that FIPS 140-2 validated cryptographic algorithms are available for the TOE to use within the operating system where the TOE is installed.
A.FIREWALL All ports needed for proper operation of the TOE will be opened at the firewall. Also, any firewall settings necessary for the TOE's operation will be configured to allow the TOE to operate.	OE.FIREWALL Any firewalls in the TOE environment must be configured such that all ports needed for the proper operation of the TOE are open and restricted from access from untrusted users. In addition, a VPN tunnel must be configured to protect the communciations between the Primary and the Remote Network.	OE.FIREWALL upholds the assumption that all ports necessary for the operation of the TOE are opened and restricted from access to untrusted users. In addition, it ensures that the communications between geographically separate locations where the TOE is installed are protected.
A.INSTALL The TOE is installed on a server platform running an operating system dedicated to the TOE and its server components.	OE.PLATFORM The TOE environment must contain the hardware and operating system upon which the TOE is installed.	OE.PLATFORM upholds this assumption by ensuring that an appropriate operating system and hardware are available for the TOE.
	NOE.MANAGE Sites depoying the TOE will provide competent, non-hostile TOE administrators	NOE.MANAGE upholds this assumption by ensuring that the TOE administrators read and follow all guidance for installation and deployment of the TOE.

Assumptions	Objectives	Rationale
	who are appropriately trained and follow all guidance.	
A.LOCATE The TOE, monitored systems, switches, monitored networks, firewall, and NTP, SMTP, and LDAP servers are located within a controlled access facility. All of the above components are installed in a Primary Network while the TOE Collector software and any combination of monitored systems may be installed in the Remote Network. Both locations share the same physical protections and access restrictions.	NOE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	NOE.PHYSICAL upholds this assumption by ensuring that the environment provides protection against physical attacks.
A.EMAIL The email accounts used by the TOE to send notifications are associated with accounts in a domain for which the TOE is also a member. Emails are not sent by the TOE to an external SMTP server, and the email server used by the TOE does not accept direct communication from external SMTP servers. Any clients, including the TOE, and those accessing the SMTP server from outside of the controlled access facility, do so using TLS.	OE.ADMIN_PROTECT The administrative and user workstations, as well as the machines hosting the TOE and its environment must be protected from any external interference or tampering.	OE.ADMIN_PROTECT upholds this assumption by ensuring that the systems in the TOE and the TOE environment are protected from external interference and tampering.
	OE.FIPS The operating system that the TOE is installed on must provide FIPS 140-2 validated cryptographic algorithms for the TOE to use to establish secure connections.	OE.FIPS upholds this assumption by ensuring that the TOE environment can provide FIPS-approved algorithms for use in establishing TLS sessions between the TOE and remote components.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	NOE.MANAGE Sites depoying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all guidance.	NOE.MANAGE upholds this assumption by ensuring that 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.
A.NETCON The TOE environment provides the network connectivity required to allow the TOE to provide secure access control monitoring functions.	OE.CONNECT The TOE environment must be implemented such that the TOE is appropriately located within and connected to the network to perform its intended function.	OE.CONNECT upholds this assumption by ensuring that the environment provides the TOE with the appropriate configuration to provide the TOE functionality.
A.NOEVIL The administrators of the TOE are non-hostile, appropriately trained, and follow all guidance. Administrators will never accept	NOE.MANAGE Sites depoying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all guidance.	NOE.MANAGE upholds this assumption by ensuring that all administrators assigned to manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.

Assumptions	Objectives	Rationale
unknown or untrusted certificates for the web or email communication with the TOE.		
A.OS_ACCESS The TOE environment is in a secure state and provides a sufficient level of protection to itself and the TOE components.	OE.OS_ACCESS The operating system upon which the TOE is installed provides a sufficient level of protection for itself and the TOE software it contains.	OE.OS_ACCESS upholds this assumption by ensuring that the OS where the TOE is installed provides enough protection for itself and the TOE to prevent tampering in a physically secure environment.
A.SECCOMM The environment provides a sufficient level of protection to secure communications between distributed TOE components and the TOE server components.	OE.SECCOMM The TOE environment must provide mechanisms to secure communications among TOE agents, probes, collectors, and the server components of the TOE.	OE.SECCOMM upholds this assumption by ensuring that the TOE environment provides adequate security to protect TOE communications.
A.TIMESTAMP The TOE environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps for the TOE.	OE.TIME upholds this assumption by ensuring that the operating system where the TOE is installed is able to provide reliable time stamps for the TOE.

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

A class of FDC requirements was created to specifically address the data monitoring and analysis functionality provided by the TOE. The audit class of the CC (FAU) was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature of the monitoring and analysis performed by the TOE, provide requirements about collecting, analyzing, storing, and reviewing collected data, and providing a separation between the TSF data (audit class) and user data collected and stored by the TOE. FDC.SCN.1 has no dependencies since the stated requirements embody all the necessary security functions. FDC_ANA.1 and FDC_STG.1 are dependent on FDC_SCN.1 since the data they make claims about must first be collected in order for it to be available for any other operations. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional assurance documentation.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended SARs defined for this evaluation.

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.

Table 16 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.AUTHENTICATE The TOE must identify and authenticate users before allowing access to any TOE functionality.	FIA_ATD.1 User attribute definition	This requirement supports O.AUTHENTICATE by requiring the TOE to store data related to login and role assignment.
	FIA_UAU.2 User authentication before any action	This requirement supports O.AUTHENTICATE by requiring the TOE to authenticate users and administrators prior to granting access to any TOE functionality.
	FIA_UID.2 User identification before any action	This requirement supports O.AUTHENTICATE by requiring the TOE to identify users and administrators prior to granting access to any TOE functionality.
O.BACKGROUND_PROCESS The TOE must be able to collect event data without causing undue strain or overuse of the CPU on systems where data collection takes place.	FRU_RSA.1 Maximum quotas	This requirement supports O.BACKGROUND_PROCESS by requiring that the TOE disables any running processes if CPU usage thresholds are exceeded.
O.DATA_TRANSFER The TOE must allow authorized users and administrators to move data across the systems on the network.	FDP_ACC.1 Subset access control	This requirement supports O.DATA_TRANSFER by defining an access control policy restricting access to functionality capable of importing and exporting monitored data.
	FDP_ACF.1 Security attribute based access control	This requirement supports O.DATA_TRANSFER by defining rules for an access control policy restricting access to functionality capable of importing and exporting monitored data.
	FDP_ETC.1 Export of user data without security attributes	This requirement supports O.DATA_TRANSFER by requiring the TOE to provide the capability to export file and ACL data to a remote system.
	FDP_ITC.1 Import of user data without security attributes	This requirement supports O.DATA_TRANSFER by requiring the TOE to provide the capability to import file and ACL data from a remote system.
	FMT_MOF.1 Management of security functions behaviour	This requirement supports O.DATA_TRANSFER by requiring the TOE to only allow authorized administrator and

Objective	Requirements Addressing the Objective	Rationale
		user roles the capability to import and export data.
	FPT_TDC.1 Inter-TSF basic TSF data consistency	This requirement supports O.DATA_TRANSFER by ensuring that the TOE is capable of transferring ACL data when transferring data between remote monitored systems.
O.LOG The TOE must record events of security relevance, provide authorized users and administrators with the ability to review the recorded events, and prevent unauthorized modification or deletion of recorded events.	FAU_GEN.1 Audit Data Generation	This requrement supports O.LOG by requiring the TOE to record events of security-relevance.
	FAU_GEN.2 User Identity Association	This requirement supports O.LOG by ensuring that the identity of a user initiating a security-relevant event is recorded along with the other event information.
	FAU_SAR.1 Audit review	This requirement supports O.LOG by requiring the TOE to provide a method to review the audit records in a human-comprehensible format.
	FAU_SAR.3 Selectable audit review	This requirement supports O.LOG by providing tools for selecting and ordering log data to enhance the capability to effectively review audit data.
	FAU_STG.1 Protected audit trail storage	This requirement supports O.LOG by preventing unauthorized modification or deletion of audit events from the log.
O.MANAGE The TOE must provide it's functionality only to authorized users and administrators in order to limit access to the security-relevant functionality of the TOE.	FDP_ACC.1 Subset access control	This requirement supports O.MANAGE by defining an access control policy restricting access to functionality capable of modifying ACL data.
	FDP_ACF.1 Security attribute based access control	This requirement supports O.MANAGE by defining rules for an access control policy restricting access to functionality capable of modifying ACL data.
	FMT_MOF.1 Management of security functions behaviour	This requirement supports O.MANAGE by requiring users and administrators to have authorized roles in order to access security-relevant TOE funcionality.
	FMT_MSA.1 Management of security attributes	This requirement supports O.MANAGE by requiring users and administrators to have authorized roles in order to access security-relevant TOE functionality.
	FMT_MSA.3 Static attribute initialisation	This requirement supports O.MANAGE by requiring secure default settings for TOE user and administrator accounts.

Objective	Requirements Addressing the Objective	Rationale
	FMT_MTD.1 Management of TSF data	This requirement supports O.MANAGE by requiring users and administrators to have authorized roles in order to access security-relevant TOE functionality.
	FMT_SMF.1 Specification of management functions	This requirement supports O.MANAGE by specifying the types of security-relevant management activities provided by the TOE.
	FMT_SMR.1 Security roles	This requirement supports O.MANAGE by specifying the roles available for user and administrator accounts.
O.MONITOR The TOE must be able to monitor machines on the network to ensure that they exist in a secure state and alert TOE users if a system enters an insecure state.	FDC_ANA.1 System Analysis	This requirement supports O.MONITOR by providing analysis functionality that allows administrators to identify insecure states within monitored systems.
	FDC_SCN.1 System Scan	This requirement supports O.MONITOR by providing the capability to gather data from monitored systems in order to identify potential insecure states.
	FDC_STG.1 Scanned Data Storage	This requirement supports O.MONITOR by ensuring that stored data from monitored systems is not vulnerable to unauthorized modification or deletion and can be archived by an authorized administrator or user.
	FDP_ACC.1 Subset access control	This requirement supports O.MONITOR by defining an access control policy restricting access to functionality capable of rolling back changes to monitored data.
	FDP_ACF.1 Security attribute based access control	This requirement supports O.MONITOR by defining rules for an access control policy restricting access to functionality capable of rolling back changes to monitored data.
	FDP_ROL.1 Basic rollback	This requirement supports O.MONITOR by providing the capability to revert changes to monitored systems before they are committed.
	FMT_MTD.1 Management of TSF data	This requirement supports O.MONITOR by providing the capability for authorized administrators to correct insecure permissions present on monitored systems.

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 process.

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.

Table 17 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	Timestamps for the TOE are provided by the environment.
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	Although FIA_UID.1 isn't claimed, FIA_UID.2, which is hierarchical to FIA_UID.1 is claimed and meets this dependency.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_ETC.1	FDP_ACC.1	✓	
FDP_ITC.1	FMT_MSA.3	✓	
	FDP_ACC.1	✓	
FDP_ROL.1	FDP_ACC.1	✓	
FIA_ATD.1	None	N/A	

SFR ID	Dependencies	Dependency Met	Rationale
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 isn't claimed, FIA_UID.2, which is hierarchical to FIA_UID.1 is claimed and meets this dependency.
FIA_UID.2	None	N/A	
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1	FMT_SMF.1	✓	
	FDP_ACC.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_SMR.1	✓	
	FMT_MSA.1	✓	
FMT_MTD.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FMT_UID.1	✓	Although FIA_UID.1 isn't claimed, FIA_UID.2, which is hierarchical to FIA_UID.1 is claimed and meets this dependency.
FPT_TDC.1	None	N/A	
FRU_RSA.1	None	N/A	
FDC_ANA.1	FDC_SCN.1	✓	
FDC_SCN.1	None	N/A	
FDC_STG.1	FDC_SCN.1	✓	

9. Acronyms and Terms

Table 18 defines the acronyms and terms used throughout this document.

Table 18 – Acronyms and Terms

Acronym	Definition
ACL	Access Control List
AD	Active Directory
API	Application Programming Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CM	Configuration Management
CPU	Central Processing Unit
DB	Database
DCF	Data Classification Framework
DGS	Data Governance Suite
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
FS	Filesystem
GB	Gigabyte
GHz	Gigahertz
ID	Identifier
IDU	Intelligent Data Usage
IIS	Internet Information Services
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MB	Megabyte
NAS	Network Attached Storage
NT	New Technology
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile

Acronym	Definition
RAM	Random Access Memory
SAR	Security Assurance Requirement
SFP	Security Functionality Policy
SFR	Security Functionality Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
UI	User Interface
VPN	Virtual Private Network

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