NetApp, Inc.

SolidFire Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes

v8.0.1.2

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.7

Prepared for:

NetApp, Inc.
495 Java Drive

Sunnyvale, CA 94089
United States of America

Phone: +1 973 548 1125
www.netapp.com

Prepared by:

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 NetApp, Inc. SolidFire Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes and will hereafter be referred to as the TOE throughout this document. The TOE is an operating system (OS) running on SolidFire storage and FC[1] nodes that provides data protection and storage management for the SolidFire Storage System. The TOE provides secure access to block level storage on the SolidFire Storage System for both iSCSI[2] and FC clients. The TOE also provides a web-based management UI[3] built upon a REST[4] API[5] with role-based access control (RBAC).

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, 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] FC– Fibre Channel
[2] iSCSI – Internet Small Computer System Interface
[3] UI – User Interface
[4] REST – Representational State Transfer
[5] API – Application Programming Interface

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 – ST and TOE References

ST Title	NetApp, Inc. SolidFire Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes Security Target
ST Version	Version 1.7
ST Author	Corsec Security, Inc.
ST Publication Date	3/8/2016
TOE Reference	NetApp, Inc. SolidFire Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes Version 8.0.1.2

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

1.3.1 SolidFire Storage System Overview

The SolidFire Storage System is a scale-out, all-flash, highly-available clustered storage system that delivers guaranteed performance for "NextGen" data centers. A cluster is made up of a collection of nodes that provide data storage and management. Each cluster of the storage system is scalable from 4-100 independent nodes providing 35 TB[6] to 3.4 PB[7] of capacity and delivering between 200,000 and 7.5M[8] guaranteed IOPS[9] to more than 100,000 volumes/applications within a single system. Each self-contained node is built on standard hardware, houses 10 SSDs[10], runs the Element OS, and is connected to other nodes in the cluster through a 10 GbE[11] network. To iSCSI and FC clients, a cluster appears on a storage network as a single logical group, represented by a virtual IP[12] (VIP) address that can be securely accessed as block storage (volumes).

Each volume within the cluster can be allocated with an exact amount of capacity and performance, which can be separately controlled. In this way performance can be managed independently of capacity. Nodes can be added or removed non-disruptively with automatic load balancing of data across the cluster, and high availability is provided with SolidFire's Helix™ RAID[13]-less data protection. These features allow for linear, predictable performance gains as the system grows, despite failure conditions.

Helix™, SolidFire's patented self-healing data protection technology provides superior storage system resiliency compared to that of a traditional RAID-based architecture. Helix automatically maintains data redundancy levels regardless of the type of failure in the system. If a node has been offline longer than 5½ minutes, Helix data protection automatically re-replicates the data by distributing it across the remaining drives and nodes within the cluster, rebuilding in minutes, versus hours or more with a traditional RAID system. If a drive fails, its data will be immediately re-replicated. By eliminating the performance variability caused by failures and facilitating non-

[6] TB – Terabyte
[7] PB – Petabyte
[8] M – Million
[9] IOPS – Input/Output Operations Per Second
[10] SSD – Solid State Drive
[11] GbE – Gigabit Ethernet
[12] IP – Internet Protocol
[13] RAID – Redundant Array of Independent Disks

disruptive handling of hardware failures and upgrades, Helix data protection delivers the predictable performance required by large-scale infrastructures for supporting firm performance service level agreements.

The key to the high availability provided by Helix data protection is a "shared-nothing" architecture. Unlike a traditional disk storage architecture with shared disk arrays, power supplies, controllers and other points of failure, there is no single point of failure in a SolidFire cluster. In fact, with Helix data protection, two copies of the same block (written to drives in 4K[14] blocks) are never stored on the same drive or node. In this way, every node in a cluster is able to contribute to redistributing the data after a failure and allows the system to withstand multiple concurrent drive failures within the same node.

SolidFire Storage System clusters are managed and provisioned through an intuitive Web-based UI called the Web UI. This UI is built upon a complete REST-based API, which itself can be used to automate storage provisioning, management, and reporting through cloud computing platforms such as OpenStack and CloudStack, as well as third-party virtualization products, such as VMware.

Other features incorporated into the SolidFire Storage System include data reduction techniques like de-duplication, compression, and thin provisioning to increase efficiency and enhance performance. In addition, snapshots of volumes and volume groups can be created to preserve a point-in-time copy of one or more volume's metadata[15] and allow volumes to be rolled back to a desired point-in-time using a very small amount of resources and storage space.

Figure 1 (below) depicts a typical 4-node SolidFire NetApp, Inc.Storage System cluster.

Figure 1 – Typical SolidFire Storage System Cluster

1.3.2 SolidFire Storage System Architecture

SolidFire Element OS 8 is the key component of the SolidFire Storage System. SolidFire Element OS 8 comes preinstalled on the SF2405, SF4805, and SF9605 storage nodes and the FC0025 FC node. The storage and FC nodes support iSCSI and FC fabrics, respectively. The FC0025 FC node provides the protocol mapping so that SCSI[16] protocols can be transported between FC clients and SolidFire storage nodes. Each node is a 1RU[17], 10-drive system, with the exception of the FC0025, which does not contain storage drives. The nodes vary in storage, memory, and CPU[18] configurations as detailed in the node specifications shown in Table 2 below.

[14] 4K – 4096 bytes
[15] Metadata is information about the data itself, e.g., where a block of data is stored on the SSD.
[16] SCSI – Small Computer System Interface
[17] RU – Rack Unit
[18] CPU – Central Processing Unit

Table 2 – Node Specifications

Node	SSD Size	Maximum Capacity (4 -100 nodes)	Maximum IOPS (4-100 nodes)	Shared Memory / Read Cache	Write Cache	CPU	Networking
SF2405	240 GB[19]	35 TB – 864 TB	200,000 – 5,000,000	64 GB	8 GB NVRAM[20]	2x 2.1 GHz[21] 6-core 15 MB[22] cache	2x 10GbE iSCSI SFP+[23] 2x 1GbE RJ45 (management)
SF4805	480 GB	69 TB – 1.7 PB	200,000 – 5,000,000	128 GB	8 GB NVRAM	2x 2.1 GHz 6-core 15 MB cache	2x 10GbE iSCSI SFP+ 2x 1GbE RJ45 (management)
SF9605	960 GB	138 TB – 3.4 PB	200,000 – 5,000,000	256 GB	8 GB NVRAM	2x 2.1 GHz 6-core 15 MB cache	2x 10GbE iSCSI SFP+ 2x 1GbE RJ45 (management)
FC0025	N/A	N/A	N/A	32 GB	N/A	2x 2.5 GHz 6-core 15 MB cache	4x 16 GB FC 4x 10GbE iSCSI SFP+ 2x 1GbE RJ45 (management)

1.4 TOE Overview

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

The software only TOE is SolidFire Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes. It is an OS running on SolidFire's storage and FC nodes that provides data protection, storage management, and block storage services for the SolidFire Storage System. Designed for large scale IT infrastructures and multi-tenant environments, it implements several key security features:

- Account (tenant) isolation – Storage is provisioned by way of volumes accessed over a storage network via iSCSI. An account is assigned to every volume. This enables iSCSI clients, or initiators, with the proper CHAP[24] account credentials to access associated volumes. Volumes may also be accessed by both iSCSI and FC clients alike with the use of volume access groups (VAGs). In this case, CHAP credentials are not required as specific mappings between IQNs [25] /WWPNs [26] and volumes, made by authorized administrators, dictate access.
- Management via the Web UI and API with RBAC – Administrators are restricted to security functions and TSF data based on their role(s).
- Multiple authentication mechanisms – Both local and LDAP[27] authentication can be configured to identify and authenticate administrators at the Web UI and API. Every API call whether direct, e.g., via scripting, or over the Web UI requires successful authentication.

[19] GB – Gigabyte
[20] NVRAM – Non-Volatile Random Access Memory
[21] GHz – Gigahertz
[22] MB – Megabyte
[23] SFP – Small Form-Factor Pluggable
[24] CHAP – Challenge-Handshake Authentication Protocol
[25] IQN – iSCSI Qualified Name
[26] WWPN – World Wide Port Name
[27] LDAP – Lightweight Directory Access Protocol

- Storage access controls – Both CHAP authentication and VAGs can be configured for storage access control. Both unidirectional and bi-directional CHAP authentication is supported.
- Data protection and fault tolerance – SolidFire's Helix data protection technology protects against user data errors and hardware failures. In addition, a suite of self-tests provide added assurance that the TOE is operating correctly.
- Auditing – Event records are created for every successful API call (excluding read-only calls, i.e., Get and List methods) and all failed API calls. Every "APIEvent" record identifies the user making the call. Event records are also generated for system level events.
- Snapshots – Snapshots of volumes and volume groups can be created to preserve a point-in-time copy of one or more volume's metadata. These snapshots can be used to roll back a volume to restore it to a desired point-in-time.
- Security attribute and TSF data management – cluster-wide configuration details and other cluster-level metadata are stored in a distributed database. The distributed database is stored independently on all nodes in the cluster. A subset of three or five cluster nodes (dependent on cluster size) is elected as voting members of the distributed database. These voting member nodes are known as the database ensemble.

1.4.1 Brief Description of the Components of the TOE

The software TOE is comprised of SolidFire Element OS 8, which is a software binary uniquely identified as version 8.0.1.2 that must be upgraded to such on the nodes shipped by SolidFire in accordance with the procedure in *SolidFire, Inc. Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes v8.0.1.2 Guidance Documentation Supplement* v1.4.

1.4.2 TOE Environment

The TOE is preinstalled on the SolidFire storage and FC nodes and is intended to be deployed in a secure data center that protects physical access to the TOE.

The TOE is deployed as part of a distributed system made up of a cluster of nodes, each running Element OS 8.0.1.2 and communicating over the Cluster network. A cluster can be any combination of 4-100 storage and FC nodes[28] (six in the case of the evaluated configuration). The TOE is supported on the following SolidFire nodes:

- SF2405
- SF4805
- SF9605
- FC0025

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

- LAN – Local Area Network
- HTTPS – Hypertext Transfer Protocol Secure
- NTP – Network Time Protocol
- TCP – Transmission Control Protocol

[28] FC nodes are deployed in sets of two.

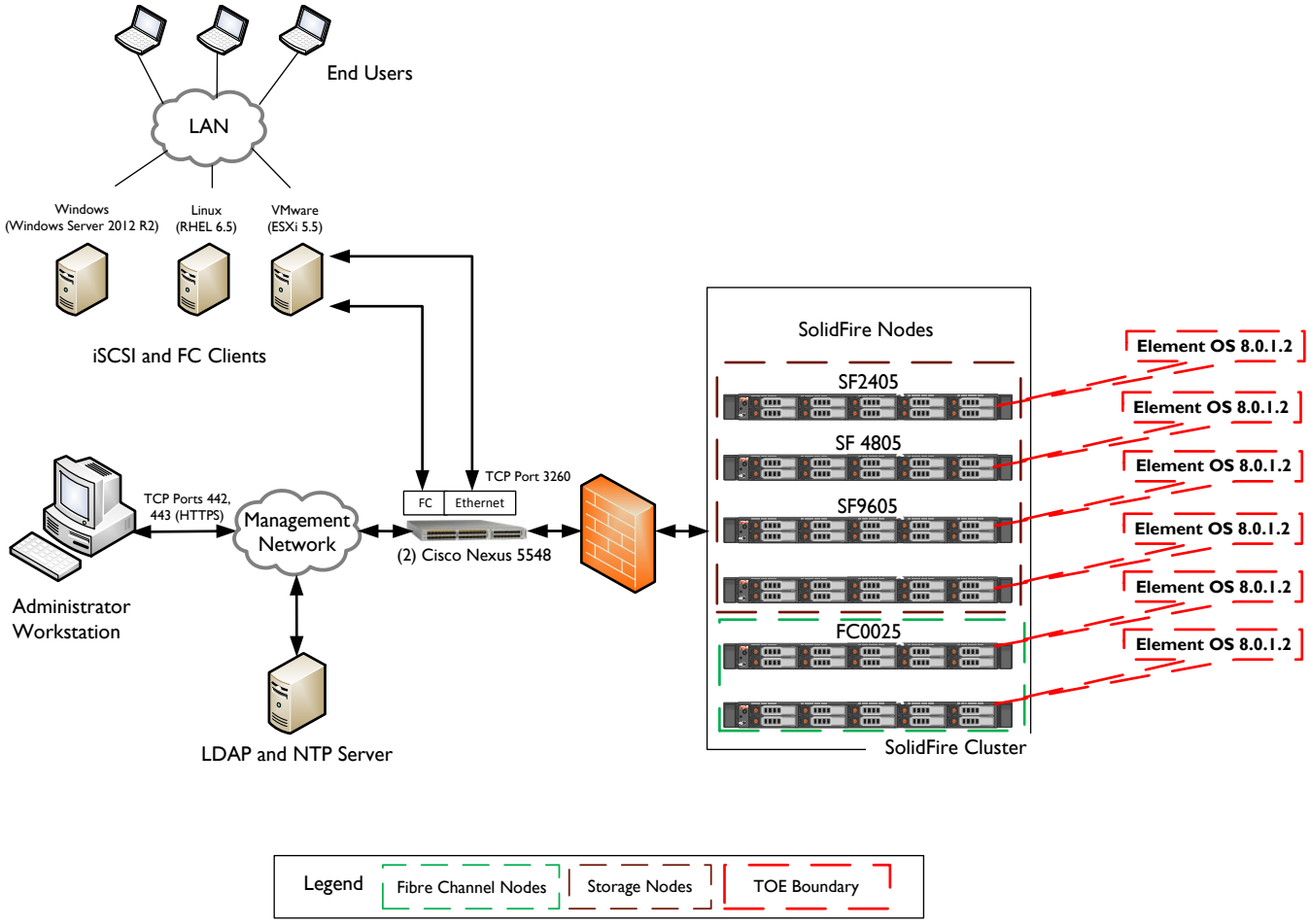

Figure 2 – Deployment Configuration of the TOE

There are four networks in the deployment configuration of the TOE: a 10 GbE network is used for iSCSI connections to clients (Storage network) and intracluster communication (Cluster network); a 1GbE management network (internal) is used for management of the TOE via the Web UI or API (Management network); and a FC storage network is used for FC connections (FC network). In the evaluated configuration, two Cisco Nexus 5548 switches are used to provide network connectivity; however other switches that meet the guidelines specified in *SolidFire Best Practices for Networking with SolidFire Storage Systems* are supported.

The cluster is presented to iSCSI and FC clients as virtual storage. A highly available storage VIP (SVIP) is the single point of access for all initial iSCSI connections. The SVIP is logically located on a node identified as a "cluster master". The node holding the cluster master role can change as a cluster operates. Upon this initial iSCSI connection to the SVIP, the cluster master sends an iSCSI redirect back to the client indicating a specific node's storage IP (SIP) that the client will use going forward for storage traffic to that specific volume.

The iSCSI and FC clients typically serve application-specific functions, e.g., hypervisor, web server, database server, mail server, file server, etc. End-user systems connect to the iSCSI and FC clients, which are located in a controlled access facility along with the TOE, through well-defined protocols. For example, an end-user accessing an iSCSI client serving as a web server may access the client via a secure channel such as HTTPS. The end-users systems connect to the clients via an Ethernet LAN. Sites deploying the TOE must ensure that the client systems are secured according to industry best practices. Communications between end-users and iSCSI and FC clients must be authenticated and encrypted.

The cluster master is also assigned a management VIP (MVIP), which is used to access a cluster over the Web UI for cluster-level management. This is done by entering the MVIP in a web browser on an administrator workstation. Each node also has a limited UI (called the Node UI) and a node-level API that listens on a separate port (442) accessible by the individual node's management IP address (MIP). An attempt to access the cluster-level Web UI or API on an individual node's MIP will redirect the browser to the cluster's MVIP.

A Text User Interface (TUI) accessible only via a directly connected console is used to initially configure nodes and establish a cluster (i.e., initial system deployment) but is excluded from further use in the evaluated configuration.

An LDAP and NTP server provide LDAP authentication and cluster time synchronization, respectively.

1.4.2.1 Non-TOE Hardware/Software

The TOE relies on non-TOE hardware/software for its essential operation. Though this hardware/software, including the SolidFire nodes, is necessary for the TOE's operation, it is not part of the TOE. The following non-TOE hardware/software is required for essential operation of the TOE:

- SolidFire Storage System hardware – a minimum of four SolidFire nodes
- Administrator workstation – used to access the Web UI and Node UI via an industry standard web browser
- Ethernet and FC switches for connections to the management and storage networks
- Cables for management and storage networks
- LDAP Server (Microsoft Active Directory (AD) Domain Services) for authentication, in one of these supported OSs: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2
- NTP Server for cluster time synchronization
- iSCSI and FC clients to connect to the cluster (evaluated with RHEL[29] 6.5, Windows Server 2012 R2, and VMware ESXi 5.5 with guest VMs[30] running RHEL 6.5 and Windows Server 2012 R2)
- Firewall - configured to protect the customer's dedicated internal management network and the client (storage) network from external interference and tampering, e.g. to protect against connections via SSH

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

The Element OS 8 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:

- Encryption At Rest – Advanced Encryption Standard 128-bit encryption is used to encrypt data on SSDs (not enabled by default).
- Integrated Backup and Restore – volumes are backed up to and restored from external object stores.
- Remote Replication – an asynchronous process is used to connect two clusters for continuous data protection.
- Remote Syslog – audit data is forwarded to a remote syslog server.
- Deduplication – multiple copies of data are replaced with references to a shared copy in order to save storage space and/or bandwidth.
- Quality of Service (QoS) – guaranteed performance is provided by setting minimum, maximum, and burst IOPS parameters for volumes.
- SSH – the SSH protocol is used by SolidFire for remote support of a customer's system (requires a Management Node, which is not part of the evaluated configuration).

[29] RHEL – Red Hat Enterprise Linux
[30] VMs – Virtual Machines

- SNMP[31]– the SNMP protocol is used by Element OS 8 to generate SNMP traps, or notifications, associated with audit events (not enabled by default).
- External API Clients and Tools (e.g., Active IQ[32], FDVA, Openstack Cinder) – external software applications and platforms are used for remote access and automated management and reporting.
- SolidFire Hardware – storage and FC nodes and SSDs are part of the SolidFire Storage System.
- TUI – this interface is used to initially configure SolidFire nodes at installation.

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 SolidFire Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes. Element OS 8 a single binary that is pre-installed on each of the storage and FC nodes shipped to a customer. The same binary is pre-installed on each node supported by the TOE. Customers may also request a copy of the software by contacting the SolidFire Support team, where they may be provided with a download link or a USB[33] key to install a new image via a return to factory image process.

1.5.1.1 TOE Software

The TOE is comprised of the Element OS software version 8.0.1.2.

1.5.1.2 Guidance Documentation

The guides listed below are required reading and part of the TOE. This SolidFire documentation (in PDF format) is available to authorized users on the SolidFire Customer Support Portal (https://system.netsuite.com) by selecting the **Knowledge Base** tab of the home page. A printed copy of the *SolidFire Storage Node Getting Started Guide* is shipped with the product.

- SolidFire Storage Node Getting Started Guide, P/N SOE-509-1150-02, REV A
- SolidFire Fibre Channel FC0025 Node - Getting Started Guide, P/N SOE-509-1150-03, REV B
- SolidFire Element 8.0 Release Notes, 06/18/2015
- SolidFire Element 8.0 User Guide, 06/10/2015
- SolidFire Element 8.0 API Reference Guide, 06/10/2015
- Configuring SolidFire on Windows for Element OS, Version:2.2, 8/10/2015
- Configuring SolidFire on Linux for Element OS, Version 2.2, 8/10/2015
- Configuring SolidFire Fibre Channel, Version: 2.0, 07/30/2015
- Best Practices for Networking with SolidFire Storage Systems, Version: 2.0.0.1, 6/11/2014
- Configuring VMware vSphere for Element OS, Version: 2.3, 5/18/2015
- SolidFire, Inc. Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes v8.0.1.2 Guidance Documentation Supplement v1.4

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.

[31] SNMP – Simple Network Management Protocol
[32] Active IQ – SolidFire's system monitoring tool.
[33] USB – Universal Serial Bus

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

1.5.2.1 Security Audit

The TOE generates audit records for events initiated by an authorized administrator through the API, Web UI, or Node UI that modify settings, as well as system level events. Authorized administrators can view the audit records through the **Reporting** tab of the Web UI; however, they are prevented from deleting the audit records. The audit records for all API events show the identity of the authorized administrator that caused the event.

The TOE maintains approximately 4,000 of the most recent log entries, meaning that the oldest records will be discarded once this threshold is reached.

1.5.2.2 User Data Protection

The TOE enforces the Storage Access Control SFP[34] to control iSCSI and FC client access to SolidFire Storage System volumes. An authorized administrator configures this access by setting security attributes (e.g., CHAP credentials, IQNs/WWPNs, VAGs) via the Web UI or API. If these security attributes are not configured, clients have no access to volumes on the SolidFire Storage System.

Data storage integrity is provided with Helix data protection, which provides built-in integrity checking and self-healing capabilities.

The TOE provides volume and volume group snapshot capabilities, allowing for the rollback of a volume or volume group to the point-in-time a chosen snapshot was created.

1.5.2.3 Identification and Authentication

User authentication can be performed in multiple ways on the TOE. SolidFire supports local and LDAP authentication. All users must be identified and authenticated prior to performing any action on the TOE's Web UI, Node UI, or API.

The TOE stores each authorized administrator's username, password, and role in the distributed database. While logging in to the Web UI and Node UI, the TOE obscures passwords for administrative users. User's credentials are cached in an administrator's web browser and passed with every API call to identify the user making the call.

1.5.2.4 Security Management

The TOE is managed by authorized administrators defined through cluster admin accounts that can be given a range of administrative permissions to perform specific tasks within a cluster. Two different cluster admin accounts are defined for the TOE: one with full access (the Administrator role); the other with read only access (the Reporting role). The same role capabilities apply to both the Web and Node UI and API. Though other roles are supported by the SolidFire product, they are seldom used and will be excluded from the evaluated configuration.

The TOE only presents users with actions permitted by their roles. The TOE provides the Administrator users with the ability to manage security functions, security attributes, and TSF data. The Reporting user has read only access and is able to view TSF data. However, Reporting users are explicitly denied access to the Node UI. They are also denied access to the Web UI **Cluster Admin** tab and parts of the Web UI **Cluster Settings** tab.

The TOE is capable of performing the following management functions: configuring clusters, volumes, and nodes; configuring NTP; viewing the Event logs; configuring user authentication; performing snapshots and rollbacks; setting access controls; and running self-tests.

[34] SFP – Security Function Policy

1.5.2.5 Protection of the TOE Security Functionality (TSF)

The TOE synchronizes its time to that of an external NTP server in the TOE environment so that it can provide time stamps for audit records to preserve the proper order of events. The internal time is managed by the TOE, and NTP is used only for periodic synchronization.

The TOE also preserves a secure state by automatically recovering when multiple drive failures on the same node or single node failures occur. Helix data protection automatically re-replicates data across all other nodes and drives in the cluster should a node or drive go offline for more than 5½ minutes. Drive and node failures are reported in the Event Log and Alerts Log.

1.5.2.6 Resource Utilization

The TOE provides limited fault tolerance in the event of multiple drive failures on the same node or a single node failure. TOE operation continues normally as data is re-replicated across all other drives and nodes in the cluster.

1.5.2.7 TSF Operational Assessment

The TOE provides a suite of self-tests to ensure the correct operation of the cluster consistency, distributed database, and network connectivity.

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 CEM as of 2015/01/30 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ Augmented with Flaw Remediation (ALC_FLR.2)

3. Security Problem

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

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

3.1 Threats to Security

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

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE administrator users: Users in charge of administration of the TOE that have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)
- FC and iSCSI clients: Users of the TOE functionality that have access to the TOE and could attempt to bypass its protection mechanisms for access to another user's data.

All users are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[35] and user data saved on or transitioning through the TOE and the hosts on the protected network. Both the confidentiality and integrity of the data must be protected. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 4 below lists the applicable threats.

Table 4 – Threats

Name	Description
T.DATA_CORRUPTION	Data could become corrupted or security functionality compromised due to hardware failure or incorrect system access by FC and iSCSI clients or attackers.
T.UNAUTH	An administrator with Reporting privileges may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.
T.UNINTENDED_ACCESS	An attacker and user of the TOE functionality (FC and iSCSI client) could access SolidFire volumes they are not authorized to access.

3.2 Organizational Security Policies

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

[35] TSF – TOE Security Functionality

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.NETWORK	The TOE environment provides the network infrastructure required for management and storage traffic.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.
A.LOCATE	The TOE, the storage nodes, storage clients, switches, storage and management networks, firewall, and NTP and LDAP servers are located within a controlled access facility.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The administrator users with Administrator privileges who manage the TOE are non-hostile, appropriately trained, and follow all guidance. Administrators will never accept unknown/untrusted certificates for the web communication with the TOE.
A.ADMIN_PROTECT	No malicious software is installed or running on the administrator workstation.

4. Security Objectives

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

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 6 below.

Table 6 – Security Objectives for the TOE

Name	Description
O.AUDIT	The TOE must record security relevant events and associate each API event with the identity of the administrator that caused the event. The TOE must prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide authorized administrators with the ability to review the audit trail.
O.ACCESS	The TOE must implement rules to govern FC and iSCSI client access to stored user data.
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions, security attributes, and TSF data, ensuring that only authorized TOE administrators (in defined roles) may exercise such control.
O.AUTHENTICATE	The TOE must be able to identify and authenticate administrators through multiple authentication mechanisms prior to allowing any access to TOE administrative functions and TSF data. An administrator's security attributes must be associated with every API and Web UI management action.
O.USER_DATA_PROTECT	The TOE must ensure the integrity of stored user data by monitoring for errors and providing the means for an authorized administrator to restore a volume (of user data) to a desired point-in-time.
O.TSF_PROTECT	The TOE must protect its functions and TSF data to ensure its SFRs are enforced and capabilities intact when drive or node failures occur. It also must provide for the ability to check that its nodes are operating correctly.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

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

Table 7 – IT Security Objectives

Name	Description
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.NETWORK	The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.
OE.SSH_PROTECT	The SSH interface to the TOE is inaccessible as it is restricted by a firewall protecting the management and client networks.
OE.ADMIN_PROTECT	The administrator workstation must be protected from any external interference or tampering.

4.2.2 Non-IT Security Objectives

Table 8 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 8 – Non-IT Security Objectives

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

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. There is one extended SFR for the TOE: TOA_TST: TSF Self Test.

5.1.1 Class TOA: TSF Operational Assessment Function

TSF Operational Assessment functions involve testing to ensure that the TSF is operating correctly and that TSF data has not been corrupted. The TOA: TSF Operational Assessment class was modeled after the CC FPT: Protection of the TSF class. The extended family TOA_TST: TSF self test was modeled after the CC family FPT_TST: TSF self test.

5.1.1.1 TSF self test (TOA_TST)

Family Behavior

This family defines the requirements for self-tests that can be carried out at start-up, periodically, or at the request of an authorized user to demonstrate the correct operation of the TSF. It also defines requirements for authorized users to be able to verify the integrity of TSF data.

Component Leveling

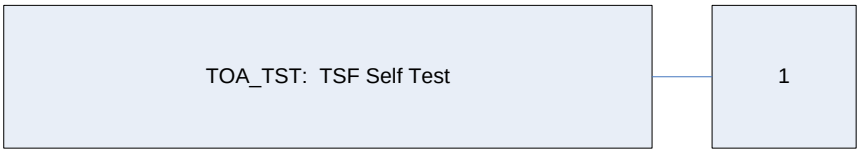

Figure 3 – TOA_TST Family Decomposition

TOA_TST.1 TSF self test, provides the capability to test the TSF's correct operation. These tests may be performed at start-up, periodically, or at the request of an authorized user. It also provides the ability for an authorized user to verify the integrity of TSF data.

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

- Authorized user execution of TSF self tests.

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

- Basic: Execution of the TSF self tests and the results of the tests.

TOA_TST.1 TSF Self Test
Hierarchical to: No other components.
Dependencies: None

TOA_TST.1.1

The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self test should occur]*] to demonstrate the correct operation of [selection: *[assignment: parts of TSF], the TSF*].

TOA_TST.1.2

The TSF shall provide authorized users with the capability to verify the integrity of [selection: *[assignment: parts of TSF data], TSF data*].

5.2 Extended TOE Security Assurance Components

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

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 [*italicized and underlined text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

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

Table 9 – TOE Security Functional Requirements

Name	*Description*	*S*	*A*	*R*	*I*
FAU_GEN.1	*Audit Data Generation*	✓	✓		
FAU_GEN.2	*User Identity Association*				
FAU_SAR.1	*Audit review*		✓		
FAU_STG.1	*Protected audit trail storage*	✓			
FAU_STG.4	*Prevention of audit data loss*	✓	✓		
FDP_ACC.1	*Subset access control*		✓		
FDP_ACF.1	*Security attribute based access control*		✓		
FDP_ROL.	*Basic rollback*		✓		
FDP_SDI.2	*Stored data integrity monitoring and action*		✓		
FIA_ATD.1	*User attribute definition*		✓		
FIA_UAU.2	*User authentication before any action*				
FIA_UAU.5	*Multiple authentication mechanisms*		✓		
FIA_UAU.7	*Protected authentication feedback*		✓		
FIA_UID.2	*User identification before any action*				

Name	*Description*	*S*	*A*	*R*	*I*
FIA_USB.1	*User subject binding*		✓		
FMT_MOF.1	*Management of security function behavior*	✓	✓		
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_FLS.1	*Failure with preservation of secure state*		✓		
FPT_STM.1	*Basic internal TSF data transfer protection*	✓			
FRU_FLT.2	*Limited fault tolerance*		✓		
TOA_TST.1	*TSF self test*	✓	✓		

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;
b. All auditable events, for the [*not specified*] level of audit; and
c. [*APIEvent, ServiceEvent, PlatformHardwareEvent, DriveEvent*].

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, [*Event ID, Message, Service ID, Node ID, Drive ID*].

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.

Application Note: ServiceEvent, PlatformHardwareEvent, and DriveEvent are not intended to be a success/fail operation; they are generated when system events occur. Therefore, there will not be a success or failure indication for these events.

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 [*Administrator and Reporting users*] with the capability to read [*all audit information for the APIEvent, ServiceEvent, PlatformHardwareEvent, DriveEvent, and start-up and shutdown events*] 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_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.

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1

The TSF shall [*overwrite the oldest stored audit records*] and [*no other actions*] if the audit trail is full.

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 [*Storage Access Control SFP*] on [
Subjects: iSCSI and FC clients
Objects: Volumes
Operations: Read and Write
].

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 [*Storage Access Control SFP*] to objects based on the following: [

1) iSCSI client SFP-relevant security attributes:
   - IQN Initiators
   - Username for CHAP authentication (i.e., account name defined on volume)
   - Initiator Secret for CHAP authentication
   - Access control record (for CHAP target authentication)

2) FC client SFP-relevant security attributes:
   - WWPN Initiators

3) Volume SFP-relevant security attributes:
   - Target Secret for CHAP authentication
   - VAG
   - Volume ID
   - Account Name (i.e., iSCSI client username)
   - Access control record (for CHAP initiator authentication)

].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*An iSCSI client can access a volume to perform read/write operations if 1) CHAP authentication is successful or 2) its initiator IQN is in the VAG defined for the volume. A FC client has similar access to a volume if its initiator WWPN is in the VAG defined for the volume.*].

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 [*no other rules*].

FDP_ROL.1 Basic rollback

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ROL.1.1

The TSF shall enforce [*Storage Access Control SFP*] to permit the rollback of the [*modifications*] on the [*data located in storage volumes*].

FDP_ROL.1.2

The TSF shall permit operations to be rolled back within the [*period of time since a chosen snapshot was created*].

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies

FDP_SDI.2.1

The TSF shall monitor user data stored in containers controlled by the TSF for [*integrity errors*] on all objects, based on the following attributes: [*checksum associated with the data*].

FDP_SDI.2.2

Upon detection of a data integrity error, the TSF shall [*stop the block service on which the data is located, repair the data from a known good copy, re-replicate the data by distributing it across the remaining drives and nodes within the cluster, and send an alert viewable via the Alert tab of the Web UI*].

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: [*username, role, and password for local authentication; LDAP users and groups and associated roles for LDAP authentication*].

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_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_UAU.5.1

The TSF shall provide [*local and LDAP authentication mechanisms*] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [*username and password provided by user matches that in distributed database (for local authentication) or LDAP (for LDAP authentication)*].

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1

The TSF shall provide only [*obscured feedback via the Web UI*] to the user while the authentication is in progress.

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.

FIA_USB.1: User-subject binding

Hierarchical to: No other components

Dependencies: FIA_ATD.1 User Attribute Definition

FIA_USB.1.1:

The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*credentials stored in user's web browser for all REST API calls, role*].

FIA_USB.1.2:

The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [*every API call will be associated with the credentials stored in the user's web browser*].

FIA_USB.1.3:

The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [*the user's credentials will remain unchanged for the duration of the API call*].

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 [*perform the actions listed in Table 10 below*] the functions [*listed in Table 10 below*] to [*the roles listed in Table 10 below*].

Table 10 – Management of Security Functions

Security Function	Actions	Role
User identification and authentication	• *Determine the behavior of* • *Modify the behavior of*	• Administrator
Rollback	• *Determine the behavior of*	• Administrator • Reporting
Rollback	• *Modify the behavior of*	• Administrator
Access Controls	• *Determine the behavior of*	• Administrator • Reporting
Access Controls	• *Modify the behavior of*	• Administrator
Self-tests	• *Determine the behavior of* • *Modify the behavior of*	• Administrator
Auditing	• *Determine the behavior of*	• Administrator • Reporting

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1

The TSF shall enforce the [*Storage Access Control SFP*] to restrict the ability to [*query, modify, delete, [add]*] the security attributes [*CHAP credentials, VAG, volume account name (modify only)*] to [*Administrator and Reporting (query only)*].

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 [*Storage 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 [*Administrator*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

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

FMT_MTD.1.1

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

Table 11 – Management of TSF Data

Operation	TSF Data	Role
Create, Modify, Delete	Volumes, accounts	Administrator
View	Volumes, accounts	Administrator , Reporting
Add, Remove	Drives, nodes	Administrator
View	Drives, nodes	Administrator, Reporting
View	FC ports	Administrator, Reporting
View	Element OS version	Administrator, Reporting
Modify	Node settings	Administrator
Add, Remove	Volumes and initiators from VAG	Administrator
Delete	VAG	Administrator
Create, delete	Snapshots, Group snapshots	Administrator
Assign, View, Modify	NTP settings	Administrator
Add, View, Delete	Cluster Admin accounts	Administrator
View	Host Connections (iSCSI and FC sessions)	Administrator, Reporting
View	Event logs	Administrator and Reporting

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: [*configuring clusters, volumes, and nodes; configuring NTP; viewing the Event logs; configuring user authentication; performing snapshots and rollbacks; setting access controls; running self-tests*].

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 [*Reporting and Administrator*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Application Note: The Administrator role (or access) provides full privileges and is obtained by selecting all access settings when the Cluster Admin account is created: Reporting, Volumes, Nodes, Accounts, Drives, and Cluster Admin. The Reporting role is read-only and is obtained by selecting the Reporting access when the Cluster Admin account is created. The Volumes, Nodes, Accounts, Drives, and Cluster Admin access settings are not used individually to create any additional roles for the TOE.

6.2.5 Class FPT: Protection of the TSF

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

The TSF shall preserve a secure state when the following types of failures occur: [*up to 10 drive failures on the same node and single node failures*].

FPT_STM.1 Reliable time stamps
Hierarchical to: No other components.
Dependencies: No dependencies
FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

6.2.6 Class FRU: Resource Utilization

FRU_FLT.2 Limited fault tolerance
Hierarchical to: FRU_FLT.1 Degraded fault tolerance
Dependencies: FPT_FLS.1 Failure with preservation of secure state
FRU_FLT.2.1

The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: [*up to 10 drive failures on the same node or a single node failure*].

6.2.7 Class TOA: TSF Operational Assessment

TOA_TST.1 TSF self test

Hierarchical to: No other components.

Dependencies: No dependencies

TOA_TST.1.1

The TSF shall run a suite of self tests [*during initial start-up, periodically during normal operation, at the request of the authorized user*] to demonstrate the correct operation of [*network connectivity, cluster consistency, distributed database*].

TOA_TST.1.2

The TSF shall provide authorized users with the capability to verify the integrity of [*TSF data stored in the distributed database*].

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 augmented with ALC_FLR.2. Table 12 – Assurance Requirements summarizes these requirements.

Table 12 – Assurance Requirements

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

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

Table 13 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_ROL.1	Basic rollback
	FDP_SDI.2	Stored data integrity monitoring and action
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
	FIA_USB.1	User subject binding
Security Management	FMT_MOF.1	Management of security functions behavior
	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
Protection of TOE Security Functionality	FPT_STM.1	Reliable time stamps
	FPT_FLS.1	Failure with preservation of secure state
Resource Utilization	FRU_FLT.2	Limited fault tolerance
TSF Operational Assessment	TOA_TST.1	TSF self test

7.1.1 Security Audit

The TOE generates audit records for events initiated by an authorized administrator through the API, Web UI, or Node UI that modify settings, as well as system level events. Authorized administrators can view the audit records in the Event Log through the **Reporting** tab of the Web UI, by extracting them with the API or pointing a web browser to https://<MVIP>/reports -> Event report; however, they are prevented from deleting the audit records. The audit records for all API events show the identity of the authorized administrator that caused the event.

The TOE maintains approximately 4,000 of the most recent log entries, meaning that the oldest records will be discarded once this threshold is reached.

The TOE generates audit records for the start-up and shutdown of the audit functions and the following event types:

- **APIEvent** – Events initiated by an authorized administrator through the API, Web UI, or Node UI that modify settings, authentication failures, and stopping services
- **ServiceEvent** – SolidFire service monitoring events, for example, starting services
- **PlatformHardwareEvent** – Events related to issues detected on hardware devices
- **DriveEvent** – Events related to drive operations

The TOE audit records contain the following information:

Table 14 – Audit Record Contents

Field	Content
Event ID[36]	Unique ID associated with each event
Event Types	The type of event being logged, for example, API events or Service events
Message	Message associated with the event
Service ID	The service that reported the event (if applicable)
Node ID	The node that reported the event (if applicable)
Drive ID	The drive that reported the event (if applicable)
Details	Information that helps identify why the event occurred
Event Time	The time the event occurred

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_STG.1, FAU_STG.4

7.1.2 User Data Protection

The TOE enforces the Storage Access Control SFP to control iSCSI and FC client access to SolidFire Storage System volumes. An authorized administrator configures this access by setting security attributes (e.g., CHAP credentials, IQNs/WWPNs, VAGs) via the Web UI or API. If these security attributes are not configured, clients have no access to volumes on the SolidFire Storage System. The TOE enforces access control to hosted volumes using accounts (CHAP authentication) and VAGs.

For account-based access control, every volume is assigned an account name (i.e., the username of the iSCSI client to whom authorized access will be granted) and associated CHAP credentials. Through an IP connection to the node holding the SVIP, an iSCSI client can access a volume to perform read/write operations if CHAP

[36] ID – Identifier

authentication is successful. For authentication to succeed, the iSCSI client username and password (initiator secret) must match that assigned to the volume. If bidirectional CHAP is configured, then the target (volume) must also authenticate with the initiator (iSCSI client). In this case, the iSCSI client must have a record of the username and password (target secret) for the volume(s) being accessed.

VAGs provide access control between a list of iSCSI initiator IQNs or FC WWPNs and an associated group of volumes. VAGs may contain volumes from more than one account. Each iSCSI initiator IQN that is added to a VAG can securely access each volume in the group without requiring CHAP authentication. Each FC WWPN that is added to a VAG will allow FC network access from that WWPN to the volumes in the VAG.

Data storage integrity is provided with Helix data protection, which provides built-in integrity checking and self-healing capabilities, as discussed in Section 1.3.1. To implement Helix, the TOE operates a block service on every drive to track the location of 4K blocks as they are written to the drive and keep checksums of the data. The TOE monitors these checksums to check for data integrity errors. If an error is encountered, the TOE will stop the block service on which the data is located, repair the data from a known good copy, re-replicate the data by distributing it across the remaining drives and nodes within the cluster, and send an alert viewable via the **Alert** tab of the Web UI.

The TOE provides volume and volume group snapshot capabilities, allowing for the rollback of a volume or volume group to a point-in-time a chosen snapshot was created.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_ROL.1, FDP_SDI.2

7.1.3 Identification and Authentication

User (administrator) authentication can be performed in multiple ways on the TOE. SolidFire supports both local and LDAP authentication.

With local authentication, administrators are authenticated using a local password-based mechanism, which authenticates and authorizes them based on their username, password, and role attributes, which are stored in the distributed database. All Web UI, Node UI, and API actions require a valid username and password combination upon invocation. Passwords are then cached within the administrator's browser and are passed to the cluster on each API call. As passwords are being entered by an administrator, the characters are masked with bullets. No functionality is available to an administrator prior to authentication.

For LDAP authentication, the TOE uses an AD server in the TOE environment to authenticate administrators.

TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UAU.7, FIA_UID.2, FIA_USB.1

7.1.4 Security Management

The TOE is managed by authorized administrators in either the Administrator or Reporting role. The same role capabilities apply to both the Web and Node UI and API. The TOE provides Administrator users with the ability to manage security attributes, and TSF data. For example, Administrator users can configure user authentication, run self-tests, and perform rollbacks. They can manage all of the security attributes required to enforce the Storage access control SFP. They are also able to manage TSF data, like creating, modifying, or deleting volumes and accounts or adding and removing volumes and initiators from a VAG.

The Reporting user has read only access and is able to determine the behavior of security functions and view TSF data. However, Reporting users are explicitly denied access to the Node UI. They are also denied access to the Web UI **Cluster Admin** tab and parts of the Web UI **Cluster Settings** tab.

The TOE is capable of performing the following management functions: configuring clusters, volumes, and nodes; configuring NTP; viewing the Event logs; configuring user authentication; performing snapshots and rollbacks; setting access controls; and running self-tests.

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

With the Helix data protection technology, the TOE is able to preserve a secure state when multiple drives on the same node or a single node as a whole fail. Helix data protection automatically re-replicates data across all other nodes and drives in the cluster should a node or drive fail. SolidFire Element OS 8 prevents two copies of the same data from being stored on the same node and ensures two copies of unique data are always kept on a cluster. Drive and node failures are reported in the Event Log.

Through a networked connection to an external NTP server, the TOE periodically synchronizes its time to an external time source. Once the TOE obtains the time from the NTP server, it maintains this time internally and uses it to provide reliable time stamps for auditing.

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

7.1.6 Resource Utilization

The TOE provides limited fault tolerance in the event of multiple drive failures on the same node or a single node failure. If a failure occurs, TOE operation continues normally as data is re-replicated across all other drives and nodes in the cluster.

TOE Security Functional Requirements Satisfied: FRU_FLT.2

7.1.7 TSF Operational Assessment

The TOE provides a suite of self-tests that that are run during initial start-up, periodically during normal operation, and at the request of an Administrator user to demonstrate the correct operation of the TOE. The consistency of the cluster and the integrity of the distributed database are checked periodically to ensure that no corruption has occurred.

To ensure a node is stable and can be brought online without issues, many tests can be executed by an Administrator user from the **System Tests** tab of the Node UI. These tests check for proper network connectivity between nodes and to the MVIP and SVIP of the cluster, the consistency of the cluster, and the integrity of the distributed database.

TOE Security Functional Requirements Satisfied: TOA_TST.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 15 below provides a mapping of the objectives to the threats they counter.

Table 15 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.DATA_CORRUPTION Data could become corrupted or security functionality compromised due to hardware failure or incorrect system access by FC and iSCSI clients or attackers.	O.AUDIT The TOE must record security relevant events and associate each API event with the identity of the administrator that caused the event. The TOE must prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide authorized administrators with the ability to review the audit trail.	The objective O.AUDIT ensures that security relevant events that may indicate attempts to tamper with the TOE are recorded.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions, security attributes, and TSF data, ensuring that only authorized TOE administrators (in defined roles) may exercise such control.	O.ADMIN supports the mitigation of this threat by ensuring that only authorized users may configure the TOE security mechanisms.
	O.USER_DATA_PROTECT The TOE must ensure the integrity of stored user data by monitoring for errors and providing the means for an authorized administrator to restore a volume (of user data) to a desired point-in-time.	The objective mitigates this threat by monitoring user data for errors and allowing rollbacks to a point-in-time.
	O.TSF_PROTECT The TOE must protect its functions and TSF data to ensure its SFRs are enforced and capabilities intact when drive or node failures occur. It also must provide for the ability to check that its nodes are operating correctly.	O.TSF_PROTECT mitigates this threat by providing mechanisms to protect the TOE data from unauthorized modification.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT ensures that the TOE is protected from external interference or tampering.

Threats	Objectives	Rationale
T.DATA_CORRUPTION Data could become corrupted or security functionality compromised due to hardware failure or incorrect system access by FC and iSCSI clients or attackers.	OE.SSH_PROTECT The SSH interface to the TOE is inaccessible as it is restricted by a firewall protecting the management and client networks.	OE.SSH_PROTECT ensures that the TOE is protected from attacks through the SSH interface by placing a firewall between administrative and storage clients and the TOE and restricting traffic only to ports necessary to management and user functions.
T.UNAUTH An administrator with Reporting privileges may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions, security attributes, and TSF data, ensuring that only authorized TOE administrators (in defined roles) may exercise such control.	The objective O.ADMIN ensures that access to TOE security data is limited to those users with access to the management functions of the TOE.
	O.AUTHENTICATE The TOE must be able to identify and authenticate administrators through multiple authentication mechanisms prior to allowing any access to TOE administrative functions and TSF data. An administrator's security attributes must be associated with every API and Web UI management action.	The objective O.AUTHENTICATE ensures that users are identified and authenticated prior to gaining any access to TOE security data.
	O.TSF_PROTECT The TOE must protect its functions and TSF data to ensure its SFRs are enforced and capabilities intact when drive or node failures occur. It also must provide for the ability to check that its nodes are operating correctly.	The objective mitigates this threat by ensuring continued operation of TOE in a secure state in the event of hardware failures.
T.UNINTENDED_ACCESS An attacker and user of the TOE functionality (FC and iSCSI client) could access SolidFire volumes they are not authorized to access.	O.AUDIT The TOE must record security relevant events and associate each API event with the identity of the administrator that caused the event. The TOE must prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide authorized administrators with the ability to review the audit trail.	The objective O.AUDIT ensures that security relevant events that may indicate attempts to tamper with the TOE are recorded.
	O.ACCESS The TOE must implement rules to govern FC and iSCSI client access to stored user data.	This objective ensures only authorized iSCSI and FC clients obtain access to TOE storage.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions, security attributes, and TSF data, ensuring that only authorized TOE administrators (in defined roles) may exercise such control.	The objective O.ADMIN ensures that only authorized users have access to TOE security data and management functionality.
	O.TSF_PROTECT The TOE must protect its functions and TSF data to ensure its SFRs are enforced and capabilities intact when drive or node failures occur. It also must provide for the ability to check that its nodes are operating correctly.	The objective mitigates this threat by ensuring continued operation of TOE in a secure state in the event of hardware failures.

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

8.2.2 Security Objectives Rationale Relating to Policies

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

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 16 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 16 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.NETWORK The TOE environment provides the network infrastructure required for management and storage traffic.	OE.NETWORK The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.	OE.NETWORK satisfies the assumption that the TOE environment will provide the appropriate connectivity to allow the TOE to perform its function.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME satisfies the assumption that the environment provides reliable timestamps to the TOE.
A.LOCATE The TOE, the storage nodes, storage clients, switches, storage and management networks, firewall, and NTP and LDAP servers are located within a controlled access facility.	OE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	Physical security is provided within the TOE environment to provide appropriate protection to the network resources. OE.PHYSICAL satisfies this assumption.
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	The TOE environment provides protection from external interference or tampering. OE.PROTECT satisfies this assumption.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	OE.MANAGE satisfies the assumption that competent individuals are assigned to manage the TOE and the TSF.
A.NOEVIL The administrator users with Administrator privileges who manage the TOE are non-hostile, appropriately trained, and follow all guidance. Administrators will never accept unknown/untrusted certificates for the web communication with the TOE.	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	OE.MANAGE satisfies the assumption that the users who manage the TOE are non-hostile, appropriately trained and follow all guidance.
A. ADMIN_PROTECT No malicious software is installed or running on the administrator workstation.	OE.ADMIN_PROTECT The administrator workstation must be protected from any external interference or tampering.	OE.ADMIN_PROTECT satisfies the assumption by ensuring that the Administrator Workstations is protected from external interference or tampering.

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 family of TOA requirements was created to specifically address the use of self tests to determine the correct operation of the TOE and the integrity of TSF data. The Protection of the TSF class (FPT) was used as a model for creating these requirements. The purpose of this family of requirements is to be able to assess that parts of the TSF are operating correctly and that TSF data has not been corrupted. 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 Security Functional Requirements in this ST.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 17 below shows a mapping of the objectives and the SFRs that support them.

Table 17 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE must implement rules to govern FC and iSCSI client access to stored user data.	FDP_ACC.1 Subset access control	The requirement meets the objective by ensuring that the Storage Access Control SFP is applied to all storage connection attempts by FC and iSCSI clients.
	FDP_ACF.1 Security attribute based access control	The requirement meets the objective by ensuring that the TOE enforces the Storage Access Control SFP on all storage connection attempts by FC and iSCSI clients.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that the TOE authenticates users prior to allowing access to administrative functions to ensure that only those trusted users may manage the security behaviour of the TOE.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by ensuring that the TOE authenticates users prior to allowing access to administrative functions to ensure that only those trusted users may manage the security behaviour of the TOE.
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions, security attributes, and TSF data, ensuring that only authorized TOE administrators (in defined roles) may exercise such control.	FMT_MOF.1 Management of security function behavior	The requirement meets the objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that the TOE restricts management of security attributes to only those users with the appropriate privileges.

Objective	Requirements Addressing the Objective	Rationale
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that the TOE restricts access to TSF data based on the user's role.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions, security attributes, and TSF data.
O.AUDIT The TOE must record security relevant events and associate each API event with the identity of the administrator that caused the event. The TOE must prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide authorized administrators with the ability to review the audit trail.	FAU_GEN.1 Audit Data Generation	The requirement meets the objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_GEN.2 User Identity Association	This requirement meets the objective by ensuring all API calls, including the Web UI and Node UI actions, are associated with the administrator that invoked the event.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides authorized administrators the ability to review logs.
	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by ensuring that the TOE protects the audit data from unauthorized deletion.
	FAU_STG.4 Prevention of audit data loss	If the audit facilities become full, the TOE ensures that only the oldest records are overwritten. This requirement meets this objective by mitigating the risk of loss of audit trail data.
	FPT_STM.1	The requirement meets the objective by providing reliable time stamps for audit records.
O.AUTHENTICATE The TOE must be able to identify and authenticate administrators through multiple authentication mechanisms prior to allowing any access to TOE administrative functions and TSF data. An administrator's security attributes must be associated with every API and Web UI management action.	FIA_ATD.1 User attribute definition	The requirement meets the objective by storing administrators' security attributes that are used for identification and authentication.
	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring each user is successfully authenticated before being allowed access to any TSF functionality.
	FIA_UAU.5 Multiple authentication mechanisms	The requirement meets the objective by providing both local and LDAP authentication mechanisms.
	FIA_UAU.7 Protected authentication feedback	The requirement meets the objective by obscuring feedback through the Web UI during authentication.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that each user is identified before being allowed access to any TSF functionality.

Objective	Requirements Addressing the Objective	Rationale
	FIA_USB.1 User subject binding	The requirement meets the objective by ensuring that every API call is associated with the user that invoked the call through the user's security attributes.
O.TSF_PROTECT The TOE must protect its functions and TSF data to ensure its SFRs are enforced and capabilities intact when drive or node failures occur. It also must provide for the ability to check that its nodes are operating correctly.	FPT_FLS.1 Failure with preservation of secure state	The requirement meets the objective by ensuring the TOE preserves a secure state upon defined drive or node hardware failures.
	TOA_TST.1 TSF self test	The requirement meets the objective by ensuring the TOE performs self-tests on TSF functions and data to detect failures.
	FRU_FLT.2 Limited fault tolerance	The requirement meets the objective by ensuring the operation of all the TOE's capabilities when defined hardware failures occur.
O.USER_DATA_PROTECT	FDP_ROL.1 Basic rollback	The requirement meets the objective by permitting rollbacks of volumes to defined points-in-time (snapshots).
	FDP_SDI.2 Stored data integrity monitoring and action	The requirement meets the objective by ensuring user data is monitored for integrity errors.

8.5.2 Security Assurance Requirements Rationale

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

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 18 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 18 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.4	FAU_STG.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_ROL.1	FDP_ACC.1	✓	
FDP_SDI.2	No dependencies	✓	
FIA_ATD.1	No dependencies	✓	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FIA_UAU.5	No dependencies	✓	
FIA_UAU.7	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2, which is hierarchical to FIA_UAU.1 is included. This satisfies this dependency.
FIA_UID.2	No dependencies	✓	
FIA_USB.1	FIA_ATD.1	✓	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FPT_FLS.1	No dependencies	✓	
FPT_STM.1	No dependencies	✓	
FRU_FLT.2	FPT_FLS.1	✓	
TOA_TST.1	No dependencies	✓	

9. Acronyms

Table 19 defines the acronyms used throughout this document.

Table 19 – Acronyms

Acronym	Definition
AD	Active Directory
API	Application Programming Interface
CC	Common Criteria
CHAP	Challenge Handshake Authentication Protocol
CM	Configuration Management
CPU	Central Processing Unit
EAL	Evaluation Assurance Level
EAR	Encryption at Rest
FC	Fibre Channel
GB	Gigabyte
GbE	Gigabit Ethernet
GHz	Gigahertz
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
IQN	iSCSI Qualified Name
iSCSI	Internet Small Computer System Interface
IOPS	Input/Output Operations Per Second
IP	Internet Protocol (Address)
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
M	Million
MB	Megabyte
MIP	Management IP
MVIP	Management Virtual IP
NTP	Network Time Protocol
NVRAM	Non-Volatile Random Access Memory
OS	Operating System
OSP	Organizational Security Policy
PB	Petabyte
PP	Protection Profile
QoS	Quality of Service

Acronym	Definition
RAID	Redundant Array of Independent Disks
REST	Representational State Transfer
RHEL	Red Hat Enterprise Linux
RU	Rack Unit
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFP+	Small Form-Factor Pluggable
SIP	Storage IP
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SSD	Solid State Drive
SSH	Secure Shell
ST	Security Target
SVIP	Storage Virtual IP
TB	Terabyte
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
TUI	Text User Interface
UI	User Interface
VAG	Volume Access Group
VIP	Virtual IP
VM	Virtual Machine
WWPN	World Wide Port Name

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