Dell Technologies, Inc.

Dell EMC VxRail Appliance 4.0

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 0.1

Prepared for:

DELL EMC

Dell Technologies, Inc.
1 Dell Way
Round Rock, TX 78682
United States of America

Phone: +1 508 435 1000
https://www.delltechnologies.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

1. Introduction 5
1.1 Purpose 5
1.2 Security Target and TOE References 5
1.3 Product Overview 6
1.4 TOE Overview 8
1.4.1 Brief Description of the Components of the TOE 10
1.4.2 TOE Environment 11
1.4.3 Product Physical/Logical Features and Functionality not included in the TOE 11
1.5 TOE Description 11
1.5.1 Physical Scope 11
1.5.2 Logical Scope 12
2. Conformance Claims 15
3. Security Problem 16
3.1 Threats to Security 16
3.2 Organizational Security Policies 17
3.3 Assumptions 17
4. Security Objectives 18
4.1 Security Objectives for the TOE 18
4.2 Security Objectives for the Operational Environment 18
4.2.1 IT Security Objectives 18
4.2.2 Non-IT Security Objectives 19
5. Extended Components 20
5.1 Conventions 20
5.2 Extended TOE Security Functional Components 20
5.2.1 Class FHA: High Availability 20
5.3 Extended TOE Security Assurance Components 21
6. Security Requirements 22
6.1 Security Functional Requirements 22
6.1.1 Class FAU: Security Audit 23
6.1.2 Class FDP: User Data Protection 24
6.1.3 Class FIA: Identification and Authentication 25
6.1.4 Class FMT: Security Management 25
6.1.5 Class FPT: Protection of the TSF 26
6.1.6 Class FRU: Resource Utilization 27
6.1.7 Class: TOE Access 27
6.1.8 Class FHA: High Availability 27
6.2 Security Assurance Requirements 27
7. TOE Summary Specification 29
7.1 TOE Security Functionality 29
7.1.1 Security Audit 30
7.1.2 User Data Protection 32
7.1.3 Identification and Authentication 32
7.1.4 Security Management 33

7.1.5 Protection of the TSF 34
7.1.6 Resource Utilization 34
7.1.7 TOE Access 35
7.1.8 High Availability 35
8. Rationale 36
8.1 Conformance Claims Rationale 36
8.2 Security Objectives Rationale 36
8.2.1 Security Objectives Rationale Relating to Threats 36
8.2.2 Security Objectives Rationale Relating to Policies 38
8.2.3 Security Objectives Rationale Relating to Assumptions 38
8.3 Rationale for Extended Security Functional Requirements 39
8.4 Rationale for Extended TOE Security Assurance Requirements 39
8.5 Security Requirements Rationale 39
8.5.1 Rationale for Security Functional Requirements of the TOE Objectives 40
8.5.2 Security Assurance Requirements Rationale 42
8.5.3 Dependency Rationale 42
9. Acronyms 44

List of Figures

Figure 1 – VxRail Appliance 6
Figure 2 – Deployment Configuration of the TOE 9
Figure 3 – FHA family decomposition 21

List of Tables

Table 1 – ST and TOE References 5
Table 2 – Model Specifications 6
Table 3 – CC and PP Conformance 15
Table 4 – Threats 16
Table 5 – Assumptions 17
Table 6 – Security Objectives for the TOE 18
Table 7 – IT Security Objectives 18
Table 8 – Non-IT Security Objectives 19
Table 9 – Extended TOE Security Functional Requirements 20
Table 10 – TOE Security Functional Requirements 22
Table 11 – Assurance Requirements 27
Table 12 – Mapping of TOE Security Functionality to Security Functional Requirements 29
Table 13 – VxRail Manager Event Record Contents 30
Table 14 – File System Audit Record Contents 30
Table 15 – File System Mystic Files Record Contents 31
Table 16 – Threats: Objectives Mapping 36
Table 17 – Assumptions: Objectives Mapping 38

Table 18 – Objectives: SFRs Mapping 40
Table 19 – Functional Requirements Dependencies 42
Table 20 – Acronyms 44

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. Dell Technologies, Inc. (Dell) develops the TOE. The TOE is the Dell EMC VxRail Appliance 4.0 and will hereafter be referred to as the TOE or VxRail throughout this document. The TOE is developed by EMC, which is a subsidiary of Dell. The TOE is a hyper-converged infrastructure appliance that provides fast and simple methods for standing up a virtualized Software-Defined Data Center (SDDC). VxRail delivers compute, network, storage, virtualization, and management for the SDDC.

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 (PP), and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 – ST and TOE References

ST Title	Dell Technologies, Inc. Dell EMC VxRail Appliance 4.0 Security Target
ST Version	Version 0.1
ST Author	Corsec Security, Inc.
ST Publication Date	September 20, 2018

TOE Reference	Dell EMC VxRail Appliance 4.0 consisting of: • VxRail Manager v4.0.400-6628128 • At least one of the following VxRail appliances: VxRail 160, 160F, E460, E460F, P470, P470F, V470, V470F, or S470 • VMware ESXi v6.0.0 build-6509460 • VMware vSAN v6.2 build 5572656

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.

VxRail appliances are built to provide all mission-critical services for a SDDC, including virtualization, compute, and storage. Full integration with VMware's vSphere, and Virtual SAN (vSAN) provide the backbone of the appliance. The appliances are deployed in clusters ranging from 4 to 16 nodes. A node provide computation for the appliance and contain multiple processors. Each 2U[1] appliance includes the 4-node base that is required for cluster operations. A single appliance can support up to 200 virtual machines (VMs). VxRail's hyper-converged infrastructure provides customer VMs with the power of an entire Storage Attached Network (SAN) in a single appliance.

Figure 1 – VxRail Appliance

Hyper-convergence is an emerging technology that refers to complete systems that provide compute resources for running a VM infrastructure and shared storage for use by VMs. Hyper-converged solutions run entirely on x86 servers with commodity internal solid-state and hard-disk drives for storage. Customers deploy the system as appliances that scale in a linear fashion; each node added to a VxRail cluster contributes a fixed amount of computational power and storage capacity. Hyper-convergence relies on software-defined storage as an underlying technology that is provided by VMware vSphere and vSAN. This software-defined storage allows the storage within individual servers to be shared across every node in a VxRail cluster.

The VxRail appliance models include four nodes in a 2U chassis. Models can include hybrid or all-flash drives.

Table 2 – Model Specifications

Model	Type of Drives	Processor	Cores per node	Raw Storage per node	Network Interface
VxRail 60	Hybrid	1 x Intel Xeon Processor	6	3.6 – 10 TB[2]	4 x 1 GbE[3] RJ45

[1] 2U – Two rack units
[2] TB – Terabytes
[3] GbE – Gigabit Ethernet

Model	Type of Drives	Processor	Cores per node	Raw Storage per node	Network Interface
VxRail 120	Hybrid	2 x Intel Xeon Processor	12	3.6 – 10 TB	2 x 10 GbE SFP+[4] or 2 x RJ45
VxRail 160	Hybrid	2 x Intel Xeon Processor	16	4.8 – 10 TB	2 x 10 GbE SFP+ or 2 x RJ45
VxRail 200	Hybrid	2 x Intel Xeon Processor	20	4.8 – 10 TB	2 x 10 GbE SFP+ or 2 x RJ45
VxRail E460	Hybrid	1 or 2 x Intel Xeon Processor	6 – 40	1.2 – 16 TB	2x10 GbE RJ45 or 2x10 GbE SFP+ or 4x1 GbE RJ45
VxRail P470	Hybrid	1 or 2 x Intel Xeon Processor	8 – 44	1.2 – 24 TB	2x10 GbE RJ45 or 2x10 GbE SFP+
VxRail V470	Hybrid	2 x Intel Xeon Processor	16 – 40	1.2 – 24 TB	2x10 GbE RJ45 or 2x10 GbE SFP+
VxRail S470	Hybrid	1 or 2 x Intel Xeon Processor	6 – 36	4 – 48 TB	2x10 GbE RJ45 or 2x10 GbE SFP+ or 4x1 GbE RJ45
VxRail 120F	All-flash	2 x Intel Xeon Processor	12	7.6 – 19 TB	2 x 10 GbE SFP+ or 2 x RJ45
VxRail 160F	All-flash	2 x Intel Xeon Processor	16	7.6 – 19 TB	2 x 10 GbE SFP+ or 2 x RJ45
VxRail 200F	All-flash	2 x Intel Xeon Processor	20	7.6 – 19 TB	2 x 10 GbE SFP+ or 2 x RJ45
VxRail 240F	All-flash	2 x Intel Xeon Processor	24	7.6 – 19 TB	2 x 10 GbE SFP+
VxRail 280F	All-flash	2 x Intel Xeon Processor	28	7.6 – 19 TB	2 x 10 GbE SFP+
VxRail E460F	All-flash	1 or 2 x Intel Xeon Processor	6 – 40	1.92 – 30.7 TB	2x10 GbE RJ45 or 2x10 GbE SFP+ or 4x1 GbE RJ45
VxRail P470F	All-flash	1 or 2 x Intel Xeon Processor	8 – 44	1.92 – 46 TB	2x10 GbE RJ45 or 2x10 GbE SFP+
VxRail V470F	All-flash	2 x Intel Xeon Processor	16 – 40	1.92 – 46 TB	2x10 GbE RJ45 or 2x10 GbE SFP+

The VxRail 160 and VxRail 160F were tested as part of this evaluation. Each nodes can optionally support a 100 Mbps[5] RJ45 management port except for the E, P, V and S series appliances, which support a 1000 Mbps RJ45 management port.

The VxRail software is the same on each appliance. VxRail appliances come with the following pre-installed:

- VxRail 4.0.400-6628128
- VMware's ESXi v6.0.0 build-6509460
- VMware's vSAN v6.2 build 5572656

[4] SFP+ – Enhanced Small Form-factor Pluggable

[5] Mbps – Megabits per second

- VMware's vCenter v6.0.0 build 6500546

Customers can use the MarketPlace within the VxRail Manager to download and install additional VMs onto the appliance.

The VxRail Manager Graphical User Interface (GUI) is used to manage the TOE. The VxRail Manager GUI provides simple deployment and configuration of VMs using the underlying VMware vSphere and vSAN components. Additionally, the GUI provides alerts and graphical representations of system health to include:

- Node, disk, and power supply failures
- Expansion status
- Health of node, appliance, and cluster to include:
  - CPU[6] usage
  - Memory usage
  - Storage IOPS[7]

VxRail provides the ability to scale-out the cluster using VMware's Loudmouth to discover all nodes and automate node configurations. Loudmouth is a proprietary implementation of zero-configuration networking technology that relies on IPv6 multicast technology to advertise and discover appliances. VMware vSAN, within the VMware ESXi's kernel, provides high-performance storage access with minimal CPU and memory overhead. vSAN pools solid state drives (SSDs) and hard disk drives (HDDs) to present hosts with a single datastore for the entire cluster. Data is then distributed and mirrored across the entire datastore according to VM-specific storage policies. These policies can determine if RAID[8], RAID-5, or RAID-6 is used to protect data, while also providing Quality of Service (QoS) capabilities on a per VM basis using a maximum IOPS. The policies are configured within vCenter and sent to the ESXi host for enforcement.

Additionally, VxRail provides a one click, graceful shutdown for the cluster ensuring that pre-checks are performed and VMs are shut down before the host shuts down. Post checks are performed after shutdowns and vSAN consistency is ensured. Restores can also be controlled by VxRail to ensure all checks are made during start-up. Deployment of VMs is also automated by VxRail. Installation and deployment of VMs from the MarketPlace use .ovf file properties to perform deployment. After the VM is deployed, VxRail can gracefully power-on the VM. Lastly, VxRail periodically scans the VMs running on the internal vCenter VM and can detect renaming, caching the latest data on the VM in the database, and perform garbage collection when a VM is removed.

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 TOE provides a software defined data center that can support hundreds virtual machines and their associated data. The TOE is a hyper-converged infrastructure hardware appliance that include VMware's ESXi as a hypervisor and a VxRail Manager virtual machine. The VMware ESXi hypervisor includes VMware's vSAN, which aggregates

[6] CPU – Central Processing Unit
[7] IOPS – Input/Output Operations per Second
[8] RAID – Redundant Array of Independent Disks

the underlying local storage to create a shared storage pool for installed VMs to use. Multiple appliances can be clustered together to extend the storage resource and provide high availability options for the stored data.

The appliances included in the TOE boundary for this evaluation includes one of the following appliances:

- VxRail 160
- VxRail 160F
- VxRail E460
- VxRail E460F
- VxRail P470
- VxRail P470F
- VxRail V470
- VxRail V470F
- VxRail S470

Figure 2 shows the details of the deployment configuration of the TOE and includes the following previously undefined acronym:

- DNS – Domain Name Service
- PSC – Platform Services Controller

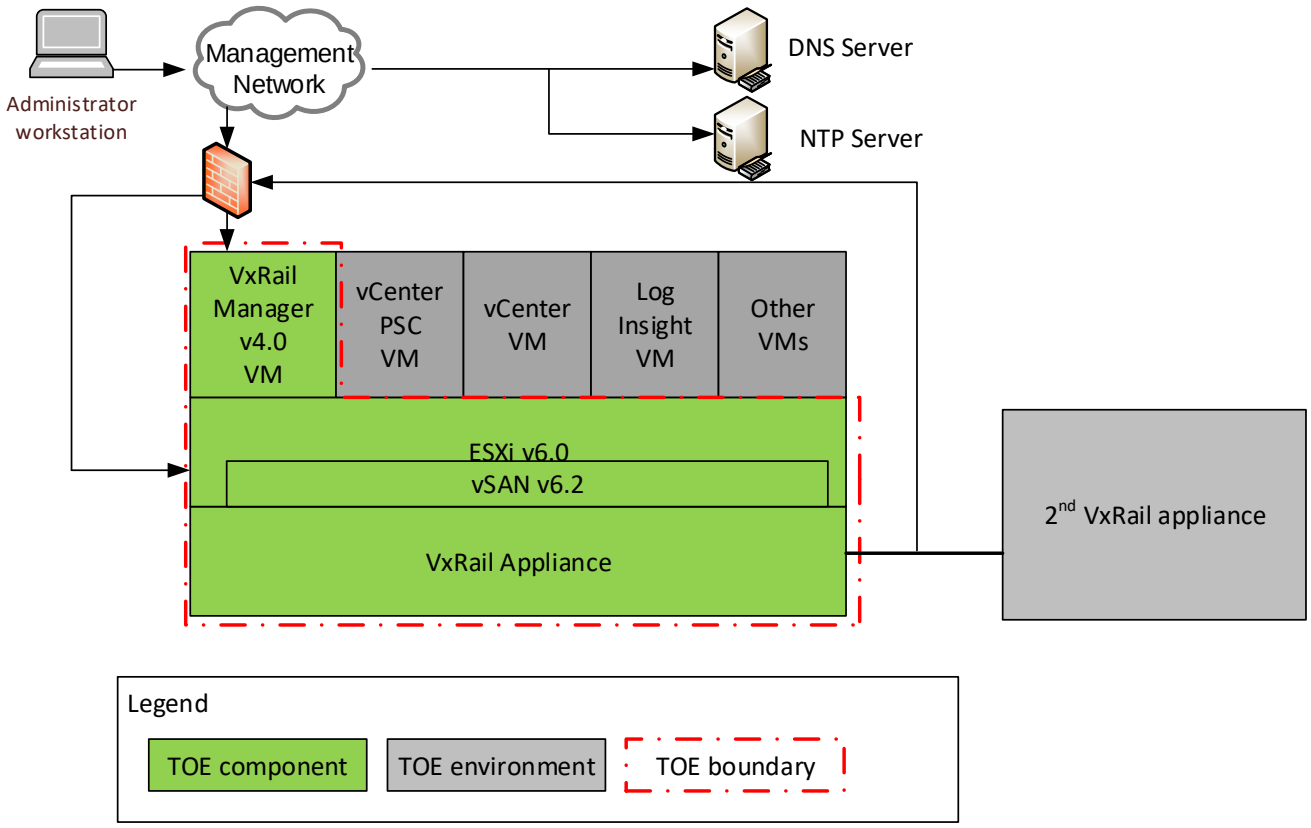

Figure 2 – Deployment Configuration of the TOE

1.4.1 Brief Description of the Components of the TOE

The TOE consists of the following components:

- VxRail Appliance – VxRail 160, 160F, E460, E460F, P470, P470F, V470, V470F, or S470 appliance
- VMware ESXi v6.0.0 build-6509460 – ESXi is the hypervisor running in the VxRail appliance. ESXi includes VMware vSAN v6.2 in its kernel.
- VxRail 4.0.400-6628128 – VxRail Manager is the software that monitors nodes, disks, power supplies, and VMs to alert an Administrator[9] to potential issues. The VxRail software includes:
    - VxRail Manager application – presents the VxRail GUI
    - SUSE Linux operating system (OS) – host OS on the VxRail VM

To verify the VMware ESXi version, log into the VMware Host Client and click on **Help -> About**. A pop-up window will show the ESXi version and build numbers. To verify the VMware vSAN version, visit https://kb.vmware.com/s/article/2150753. The page shows mappings of ESXi version to vSAN versions. The ESXi build-6509460 maps to the ESXi v6.0 Patch 5 version and includes the vSAN build-5572656.

The TOE boundary does not include customer supplied VMs or any external components such as a DNS server or network infrastructure. VMware vCenter is also excluded from the boundary. Though not included in the TOE boundary, all components are required in the TOE environment.

Administrators of the TOE can access security services through four interfaces: VxRail Manager GUI, Linux Shell Interface, vSphere API[10], and VMware Host Client.

- VxRail Manager GUI – The VxRail Manager GUI provides statistics and alerts about monitored hardware, networks, and VMs as well as functionality to power down the appliance and deploy VMs.
- Linux Shell Interface – The Linux Shell Interface provides limited access to the host OS on the VxRail Manager VM. Authorized Administrators can access audit logs through this interface and power off the VxRail Manager VM.
- vSphere API – The vCenter VM in the TOE environment uses the vSphere API for communicating storage policies and VM configurations to the ESXi hypervisor. The vSphere Web API is also an exposed web service running on both the vCenter VM and on each ESXi host. In the evaluated configuration is recommended that only the vSphere API on the vCenter Server be used to maintain consistency on all ESXi hosts.
- VMware Host Client – Each ESXi host maintains a VMware Host Client interface that can be used to manage the single ESXi host. In the evaluated configuration it is recommended that this interface only be used for emergency management when vCenter Server is unavailable.

Each ESXi node offers a vSphere Web UI and access to the vSphere API, but these should not be used for administrative actions. The nodes should be administered through vCenter. The TOE can be deployed in various configurations from a single appliance to multiple appliances clustered across physically separate datacenters. The configurations for this CC evaluation will be as a single appliance and with two appliances clustered together.

[9] Note that an Administrator is a person using the TOE with an account that has either the Administrator or CLI Root roles assigned to it. The vCenter System role is also and administrative account, but is a system role. When the term User is used, it refers to the VMs and users of the VMs that access the TOE resources.

[10] API – Application Programming Interface

1.4.2 TOE Environment

The TOE relies on non-TOE hardware/software for its essential operation. Though this hardware/software 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:

- VMware vCenter Server – The TOE is delivered with vCenter pre-installed on the VxRail appliance. The TOE relies on vCenter for authentication, creation of storage policies, and to maintain the list of VMs installed on the appliance. The vCenter component consists of two VMs on the appliance.
- DNS server – A DNS server is required for network address resolution.
- NTP server – An NTP server is required as a time source.
- Customer installed VMs – The TOE provides virtualization and storage for customer VMs to suit their business needs. An arbitrary number of VMs can be deployed, not exceeding the physical resources provided by the TOE.
- Firewall – A firewall protects the TOE interfaces.
- At least one 10GbE network switch with eight switch ports is also required to provide network switching for the TOE.
- Cabling – the following cables or equivalent are required for each type of port:
    - RJ45 Network Interface Cards (NIC) ports – 2 x CAT6 or higher cables per node which are shipped with the TOE
    - SFP+ NIC ports – 2 x compatible twinax DAC cables per node or 2 x fiber cables per node
- Administrator workstation – This workstation is used to access the VxRail GUI via an industry-standard browser.

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

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

- N/A

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 deployed on VxRail 160, 160F, E460, E460F, P470, P470F, V470, V470F, or S470 as a hyper-converged infrastructure appliance. EMC Professional Services delivers and sets up the TOE at customer sites.

1.5.1.1 TOE Hardware and Software

The TOE is an appliance with ESXi v6.0, vSAN v6.2, and VxRail Manager 4.0.400-6628128 that provides all mission-critical services for a SDDC, including virtualization, compute, and storage. Each 2U appliance includes the 4-node base that is required for the cluster operations. A single appliance can support up to 200 VMs. All software components are pre-installed on the appliance prior to shipment to customers.

The TOE's functionality is the same regardless of the hardware appliance on which they are installed. The software varies only according to low-level driver differences needed for the different appliance models.

1.5.1.2 Guidance Documentation

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

- *Dell EMC VxRail Appliance Version 4.0 Administration Guide,* REV 01
- *Administering VMware Virtual SAN,* Virtual SAN 6.2, EN-002061-03, VMware
- *VMware Virtual SAN 6.2 Release Notes,* Updated on: 24 February 2017, 15 March 2016
- *vSphere Virtual Machine Administration,* Update 1, ESXi 6.0, vCenter Server 6.0, EN-001887-04, VMware
- *vSphere Web Services SDK Programming Guide vSphere Web Services SDK 6.0,* EN-001411-02, VMware
- *vSphere Single Host Management – VMware Host Client,* Update 2, VMware vSphere 6.0, VMware ESXi 6.0, VMware Host Client 1.4, EN-001982-00, VMware
- *Dell Technologies, Inc. Dell EMC VxRail Appliance 4.0 Guidance Documentation Supplement, Evaluation Assurance Level (EAL): EAL2+*, Document Version: 0.1

The Dell documentation is provided in PDF format to customers via the EMC Support site (emc.com/vxrailsupport). VMware's documentation can be found online at https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html. A printed copy of *Dell EMC VxRail™ Appliance Version 4.0, Administration Guide,* REV 01 is delivered with the TOE.

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
- TOE Access
- High Availability

1.5.2.1 Security Audit

The TOE generates audit records and stores them in the VxRail Manager filesystem. Each log type has a maximum file size and maximum number of files that are saved. If all files become full, the oldest file is overwritten with a

new log file. Audit events include startup and shutdown of the appliance, disk failures, node failures, and authentication events. The log file is protected from unauthorized deletion and modification. Only an authorized Administrator can modify or delete these files.

1.5.2.2 User Data Protection

The TOE uses a VM-centric data access approach defined by the Virtual Disk Access SFP. VMs are assigned a virtual disk when created. The TOE ensures that VMs can only access files stored in their assigned virtual disk. Additionally, the ESXi processes can access files to distribute the data according to the VM's defined storage policy.

The TOE monitors the stored data for integrity errors using an end-to-end checksum. If an error is detected, the TOE will attempt to repair the data, update the disk statistics, and record an event in the event log.

1.5.2.3 Identification and Authentication

The TOE requires Administrators to identify and authenticate themselves prior to accessing the TSF. The TOE relies on vCenter's Single Sign-On (SSO) service to authenticate Administrators. Rules for creating usernames and passwords are determined by policies established in vSphere. When an Administrator enters their password, the TSF provides obscured feedback on its interfaces.

1.5.2.4 Security Management

The TOE provides the Administrator, vCenter System, ESXi Root, and CLI[11] Root roles. The Administrator role has access to the VxRail Manager GUI and can perform system monitoring, deploy a VM, and gracefully shutdowns of VMs. The CLI Root role has access to the Linux shell interface to view information and submit commands and can access log files. The vCenter Server is provided the vCenter System role within ESXi to communicate storage policies and VM configurations. Storage policies are restrictive by default and can only be modified in vCenter and sent to the TOE using the proxy account. Both the Administrator and vCenter proxy account can change a VM name. The ESXi Root role is used to access individual ESXi hosts for maintenance purposes and troubleshooting only.

1.5.2.5 Protection of the TSF

The TOE will maintain a secure state when disk read errors cause various disks on a node to fail. Different storage policies can be set for each VM, allowing the protection level to vary per VM. VxRail monitors the appliances' power supplies, nodes, and disks to ensure they are operational and it will show an alert in the VxRail Manager GUI if an error is detected. The TOE also performs a set of network tests during initial setup and when additional storage is added. The host OS provides a reliable timestamp for the TOE.

TSF data is sent from the vCenter VM to the ESXi hypervisor for enforcement of the storage policies and VM configurations. The TOE consistently interprets this data by ensuring that available CPU, storage, and network data is sent to vCenter. The TOE verifies that vCenter does not allocate more than the available resources for these components when it receives updates. When an update is sent, the TOE will replace any previous data with the updated data.

1.5.2.6 Resource Utilization

The TOE provides continuous functionality when disk read errors cause various disks on a node to fail. Increased fault tolerance can be assigned to individual VMs. The TSF can enforce maximum size restrictions on VMs.

[11] CLI – Command Line Interface

1.5.2.7 TOE Access

The TOE's interfaces provide Administrators with an option to log out and end the session. This prevents the session from sitting open when the Administrator is not at their workstation.

1.5.2.8 High Availability

The TOE monitors underlying disks, networks, and nodes to determine overall health and statistics on these components. Alerts are shown on the VxRail Manager GUI if a component fails or is in a degraded state. Additionally, if a disk has been improperly removed an alert is shown.

2. Conformance Claims

This section and Table 3 provide the identification for any CC, 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 September 20, 2018 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	2+ augmented, (Augmented with Flaw Reporting Procedures (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 two categories:

- Attackers or Users who are not Administrators: 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.
- Administrators: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (Administrators are, however, assumed not to be willfully hostile to the TOE.)

All are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[12] 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 below. Table 4 below lists the applicable threats.

Table 4 – Threats

Name	Description
T.AUDIT_COMPROMISE	An attacker may cause audit records to be lost or modified or prevent future records from being recorded, thus masking an Administrator's actions.
T.DATA_CORRUPTION	An attacker may cause data to become corrupt or compromise TOE security due to hardware failure.
T.EXPLOIT	An attacker may attempt to gain unauthorized access to the resources of the managed devices by exploiting vulnerabilities on a managed device.
T.UNAUTHORIZED _ACCESS	An Administrator or User may gain unauthorized access (view, modify, or delete) to user data.

[12] TSF – TOE Security Functionality

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.

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_AUTH	The TOE environment provides a secure repository of Administrators that are authorized to manage the TOE.
A.ADMIN_PROTECT	The TOE environment provides the workstation used to manage the TOE that is free of malicious software.
A.NETWORK	The TOE environment provides the routers, switches, cabling, connectors, and firewalls required for its operation and to ensure the TOE is secured and protected from interference or tampering.
A.NOEVIL	The Administrators who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.PHYSICAL	The TOE hardware, data it contains, firewalls, and 10 GbE switch are assumed to be located in a physically secure facility.
A.PROTECT	The TOE software will be protected from unauthorized modification.

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.ACCESS	The TOE must enforce an access control policy in order to prevent unauthorized Users from gaining access to user data stored on the TOE. The TOE must also provide accessing Administrators with the ability to manage the TOE and its security attributes. Any Administrator accessing the TOE will be associated to a role.
O.AUDIT	The TOE will provide the capability to detect security relevant events and create records of those events in the audit trail. These events must be protected from unauthorized modification and overwrite the oldest stored audit records once the log is full.
O.AUTHENTICATE	The TOE must be able to identify and authenticate Administrators prior to allowing any access to TOE administrative functions and TSF data. The TOE must also provide mechanisms to visually protect passwords during authentication, verify that passwords meet the complexity requirements, and to end the current session while logged into the TOE.
O.TSF_PROTECT	The TOE must protect its functions and TSF data to ensure its data and capabilities are intact when a disk read error causes a drive or node to fail. It also must provide the ability to check that its nodes, disks, and storage network are operating correctly.
O.USER_DATA_PROTECT	The TOE must ensure the integrity of stored user data by monitoring for errors and automatically correcting the errors. The TOE must also ensure that denial of service will not occur because of unauthorized monopolization of resources.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

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

Table 7 – IT Security Objectives

Name	Description
OE.ADMIN_PROTECT	The Administrator workstation must be protected from any external interference or tampering.

Name	Description
OE.AUTH	The TOE environment must provide a secure repository of Administrator accounts used to manage the TOE.
OE.NETWORK	The routers, switches, cabling, connectors, and firewalls on which the TOE is attached must be properly implemented such that the TOE is secured and protected from interference or tampering.
OE.PROTECT	The TOE environment must protect itself and the TOE from 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
NOE.PHYSICAL	A secure access facility must protect the physical security of the TOE, data it contains, firewalls, 10GbE, and the TOE environment.
NOE.TRUSTED_ADMIN	Administrators are trusted to follow and apply all administrative guidance in a trusted manner.

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 5.1.

5.1 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.

5.2 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
FHA_TST.1	System Testing

5.2.1 Class FHA: High Availability

The High Availability class ensures that the TOE provides high availability capabilities to minimize the downtime experienced in the event of an error. The FHA: High Availability function class was modeled after the CC FPT: Protection of the TSF class. The extended family FHA_TST: System Testing was modeled after the CC family FPT_TST: TSF self-test.

5.2.1.1 System Testing (FHA_TST)

Family Behavior

This family defines the requirements for high availability tests that should be available to assist in determining if there has been an error that hampers the proper functioning of the TOE.

Component Leveling

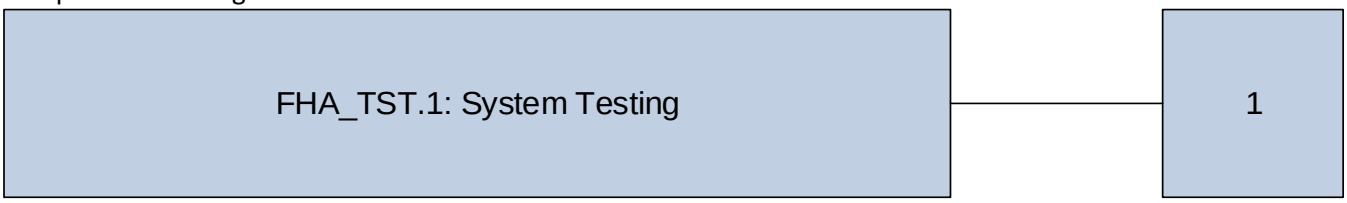

Figure 3 – FHA family decomposition

FHA_TST: System Testing provides the capability for the TOE to perform tests on assigned functions to ensure its proper function.

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

- Management of the high availability settings for the TOE.

Audit: FHA_TST.1
There are no auditable events foreseen.

FHA_TST.1 System Testing
Hierarchical to: No other components
FHA_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 administrator [assignment: *administrator roles with this privildge*], at the conditions [assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of [assignment: *functionality covered by self tests*].
Dependencies: No dependencies

5.3 Extended TOE Security Assurance Components

There are no extended SARs defined for the TOE.

6. Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 5.1.

6.1 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_STG.1	Protected audit trail	✓			
FAU_STG.4	Prevention of audit data loss	✓	✓		
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FDP_SDI.2	Stored data integrity		✓		
FIA_UAU.2	User authentication before any action				
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UID.2	User identification before any action				
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_FLS.1	Failure with preservation of secure state		✓		
FPT_STM.1	Reliable time stamps				
FPT_TDC.1	Inter-TSF basic TSF data consistency		✓		
FRU_FLT.2	Limited fault tolerance		✓		
FRU_RSA.1	Maximum quotas	✓	✓		
FTA_SSL.4	User-initiated termination				
FHA_TST.1	TSF health testing	✓	✓		

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

6.1.1 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. [
    a. *Successful Administrator login and logouts* at VxRail Manager GUI
    b. *Successful login and logout at VxRail CLI shell*
    c. *Authentication failures at VxRail Manager GUI and CLI shell*
    d. *Disk failure*
    e. *Node failure*

    ].

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*[13]*, Event Code, Severity, Appliance, Component, Component ID, ESXi Host, Message, and Time or In file system logs: Timestamp, Type, msg, success, uid, comm*].

Note: Successful administrator login and logouts at VxRail Manager GUI will require a minimum of 30 minutes' interval for generating an audit record. All failed authentication attempts at VxRail Manager GUI generate an audit record.

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 action*] if the audit trail is full.

[13] ID – Identification

6.1.2 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 [*Virtual Data Access SFP*] on: [
Subjects
- *VMs*
- *ESXi process*

Objects
- *VM disks*

Operations
- *read*
- *write*
- *move*

].

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 [*Virtual Data Access SFP*] to objects based on the following: [
Subjects
- *VM: VM name, assigned VM storage policy*
- *ESXi process: process name*

Objects
- *Virtual disk name*
- *File type*

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*A VM (identified by the VM name) can access stored data if the data is stored within the VM's assigned virtual disk (identified by the virtual disk name). Otherwise, access is denied.*]

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*ESXi process (vMotion) can move or rename stored data to meet the VM's assigned storage policy.*]

FDP_ACF.1.4

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

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: [*checksums of data*].

FDP_SDI.2.2

Upon detection of a data integrity error, the TSF shall [*repair the data or report the error*].

6.1.3 Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identifications

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.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*] 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.

6.1.4 Class FMT: Security Management

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 [*Virtual Disk Access SFP*] to restrict the ability to [*change_default, modify, delete*] the security attributes [*VM name, and assigned storage policy; file name and file type*] to [*vCenter System role*].

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 [*Virtual Disk Access 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 [*vCenter System role*] to specify alternative initial values to override the default values when an object or information is created.

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: [*monitor system health, deploy and shut down VMs, assign management IP[14] address for VM*].

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 [*Administrator, vCenter System, and CLI Root, and ESXi Root*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.1.5 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: [*disk read errors that result in the failure of all disks on a node, multiple disks on a node, or one disk on a node*].

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.

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 [*storage policies and VM configurations*] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2

The TSF shall use [

- *only the system account assigned to vCenter System role to change the policies and configurations*
- *requested configurations are checked against resource availability and are not applied if they exceed resource availability*

] when interpreting the TSF data from another trusted IT product.

[14] IP – Internet Protocol

6.1.6 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: [*disk read errors that result in the failure of all disks on a node, multiple disks on a node, or one disk on a node*].

FRU_RSA.1 Maximum quotas
Hierarchical to: No other components.
Dependencies: No dependencies
FRU_RSA.1.1

The TSF shall assign maximum quotas of the following resources: [*VMDK file*] that [*subjects*] can use [*Simultaneously*].

6.1.7 Class: TOE Access

FTA_SSL.4 User-initiated termination
Hierarchical to: No other components.
Dependencies: No dependencies
FTA_SSL.4.1

The TSF shall allow user-initiated termination of the user's own interactive session.

6.1.8 Class FHA: High Availability

FHA_TST.1 System testing
Hierarchical to: No other components
Dependencies: No dependencies
FHA_TST.1.1

The TSF shall run a suite of self tests [*periodically during normal operation, at the request of the authorized administrator* [*with Administrator role*]] to demonstrate the correct operation of the [*nodes, disks, and storage network*].

6.2 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

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

7. TOE Summary Specification

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

7.1 TOE Security 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_STG.1	Protected audit trail
	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_SDI.2	Stored data integrity
Identification and Authentication	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_FLS.1	Failure with preservation of secure state
	FPT_STM.1	Reliable time stamps
	FPT_TDC.1	Inter-TSF basic TSF data consistency
Resource Utilization	FRU_FLT.2	Limited fault tolerance
	FRU_RSA.1	Maximum quotas
TOE Access	FTA_SSL.4	User-initiated termination
High Availability	FHA_TST.1	TSF health testing

7.1.1 Security Audit

The TOE generates audit records and stores them within the filesystem in the VxRail Manager VM. The VxRail Event log audits disk failures, node failures, and authentication events. Administrator login and logouts at the VxRail Manager GUI generate an audit record. Successful administrator login and logouts at VxRail Manager GUI will require a minimum of 30 minutes' interval for generating an audit record. All failed authentication at VxRail Manager GUI attempts generate an audit record. These logs are found on the **Events** page of the VxRail Manager GUI and include the content detail in Table 13.

Table 13 – VxRail Manager Event Record Contents

Field	Content
Timestamp	Contains the date and time the event occurred.
Event ID	An auto-generated code that is unique for each event.
Event Code	A code that maps to a specific event definition. MYSTIC11C002: User login succeeded MYSTIC114002: User login failed MYSTIC11C003: User logout MYSTIC028005: Hardware health changed – node status MYSTIC014000: Cluster health - Error
Severity	Defined severity level of the event. Options include Info, Warning, Notice, Alert, Critical, and Error.
Appliance	Lists which appliance the event came from, if applicable.
Component	Lists the component name where the event came occurred if applicable.
Component ID	Lists a unique ID for the component on which the event occurred, if applicable.
ESXi Host	Lists the host name for the ESXi hypervisor where the event occurred, if applicable.
Message	Verbose text for event that includes success or failure.

Additional audit logs are generated and stored in the VxRail Manager file system. These are accessible only through the VxRail Manager CLI. In particular, audits of system startup and shutdown and logins and logouts to the VxRail Manager CLI, are recorded in /var/log in the filesystem. Audit functions are implicitly started at the startup of the appliance and close at application shutdown, therefore audits of appliance startup and application shutdown are used to show start-up and shutdown of audit functions. The audit records on the file system should be viewed using `ausearch` or `aureport`.

CLI successful and unsuccessful logins and logout are recorded in /var/log/audit. This file contains the record types listed in Table 14.

Table 14 – File System Audit Record Contents

Field	Content
Timestamp	Contains the date and time the event occurred.
Type	Contains the type of event, such as USER_AUTH, USER_LOGIN, USER_LOGOUT
msg	This field contains a time stamp and a unique ID for the record in the form audit (time stamp: ID). Multiple records can share the same time stamp and ID if they were generated as part of the same audit event.
success	This value can be 'yes' or 'no' and determines if the recorded event was successful

Field	Content
auid	This is the users audit ID. It is assigned to each user upon login and is inherited by every process invoked by the user.
uid	This is the user ID of the user who invoked the process.
comm	Records the command-line name of the command that was used to invoke the analyzed process.

Events related to the appliance startup and shutdown are recorded in /var/log/mystic/connectors-cluster.log. Examples of these events include:

- Shutdown: `Starting to shut down VxRail Manager`
- Startup: `ClusterMain.main:35 - Application Context initializing…`

All log files within the /var/log/mystic folder contain the record contents detailed in Table 15.

Table 15 – File System Mystic Files Record Contents

Field	Content
Timestamp	Contains the date and time the event occurred.
Level	The level of log message that is recorded. Possible values are INFO, DEBUG, ERROR, of WARN
Process	This field is in brackets [ ] and contains details on the process that initiated the action.
Message	This field includes a detailed message on what action occurred, including its success or failure.

All logs are protected from unauthorized deletion and modification. Only an authorized Administrator can modify or delete these files. Each log file has a different rotation configuration. These configurations are:

- /var/log/mystic files (except /var/log/mystic/hibernate and /var/log/mystic/management-account)
  - Maximum size is 50MB
  - Logs are rotated after 20 files are filled
  - No maximum age
- /var/log/mystic/hibernate.log
  - Maximum size is 50MB
  - Logs are rotated after 10 files are filled
  - No maximum age
- /var/log/mystic/management-account.log
  - Maximum size is 11MB
  - Logs are rotated after 2 files are filled
  - No maximum age
- /var/log/audit.log
  - Maximum size is 11 MB
  - Logs are rotated after 1 file is filled
  - No maximum age

Additionally, the /var/log/audit.log file is saved daily until the folder reaches a total of 50MB. Once the /var/log/audit folder reaches 50MB the oldest daily audit.log file is deleted.

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

7.1.2 User Data Protection

The TOE uses VMware vSAN's VM-centric storage policies to provide access control for VMs accessing the local storage. These policies make up the Virtual Disk Access SFP and include fault protection and Quality of Service (QoS) policies as well. VMs are identified by their name. Each VM is assigned to a defined virtual storage policy. Since vSAN abstracts all storage into a single pool of storage, the storage resources are defined by their file name and file type. Every file related to a particular VM is stored in that VM's assigned virtual disk. The file type determines what type of VM data is stored there. Virtual machine file types can include:

- .vmx – The VM configuration file includes metadata on the VM and its configurations.
- .vmdk – The virtual disk characteristics file includes the VM's file system.
- .vmsd – The virtual machine snapshot metadata includes all information on snapshots that have been taken of the VM's .vmdk file.
- .vswp – The VM swap file is created when the VM is powered on and serves as a backup for the VM's RAM[15] contents.
- .vmss – The VM suspend file contains metadata on a VM's state at the time the VM was suspended.

The Virtual Disk Access SFP ensures that only the VMs are able to discover the virtual disk (.vdmk file) that is assigned to them. VMs cannot discover or access a different VM's virtual disk. ESXi processes must also have access to these files to rename and move the files according to the VM's assigned storage policy.

ESXi processes will use the VM's storage policy to determine which storage resources should be used to store the VM's data and if the data requires mirroring or replication. If a VM is renamed or moved to another cluster, the ESXi process, vMotion, will rename and move all VM files as well.

The TSF monitors data for integrity errors using an end-to-end checksum that is verified during read and write operations. If an error is detected, the TOE will automatically attempt to repair the data. The disk statistics in the VxRail Manager GUI are updated and an event is recorded with the error count.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FCP_ACF.1, and FDP_SDI.2.

7.1.3 Identification and Authentication

Administrators of the TOE are required to enter a username and password on the VxRail Manager GUI prior to gaining access to the GUI. VxRail sends the username and password to the vCenter SSO service in the TOE environment. The vCenter VM resides on the VxRail appliance but is outside the TOE boundary. The vCenter PSC VM verifies the password and returns the Administrator's role if the verification is a success. If the password verification is a failure, the vCenter PSC VM returns a failure to the TOE. The Administrator is only allowed access to the REST API prior to the TOE receiving verification of the password from vCenter. The Administrator's account ID is then used by the TOE, along with the Administrator's role, to determine access to TSF functionality.

[15] RAM – Random Access Memory

Access to the Linux Shell interface can only be obtained through vCenter. When an administrator opens a console interface they are directed to the Linux Shell login page. No access to the shell is allowed prior to login. Lastly, the individual ESXi hosts offer a UI that administrator must authenticate to prior to access. This interface also relies on the vCenter PSC for verification.

TOE interfaces VxRail Manager GUI, ESXI UI, and vSphere API show dots (•) while the Administrator is typing the password instead of the characters. The password is obscured using space character on the Linux Shell Interface.

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

7.1.4 Security Management

The TOE provides the following roles:

- Administrator role – The Administrator role is part of the Administrator group in vCenter and has access to the VxRail Manager GUI and can perform administrative tasks on the VxRail Manager GUI including deploying and powering down VMs.. All commands available on the VxRail GUI are available to this role.
- vCenter System role – The vCenter System role is used by vCenter PSC to communicate storage policies and VM configurations within ESXi. This system role sends commands entered by administrators on vCenter to the TOE. This role has access to the vSphere API to manage VMs and their related storage policies. No additional administrators can be added to this role. Commands entered on the vSphere Web Client by any vCenter user or administrator are translated by the vCenter VM into vSphere API calls and sent to the TOE.
- CLI Root role – The CLI Root role is used to access the authenticated Linux shell interface where the Administrator can browse the various menus and buttons available to view information and submit commands.
- ESXi Root role – The ESXi Root role is used to access individual ESXi hosts for maintenance purposes and troubleshooting. This role can only manage the individual host on which it has authenticated.

The default storage policies are restrictive ensuring that VMs can only access data that is associated with their VM. The hypervisor applies a default storage policy to all VMs unless a specific storage policy is created. The Administrator must assign a VM name when creating the VM. If the VM is created using the vCenter VM, then the VM name, its associated virtual disk name, and any VM-specific storage policies must be sent to the ESXi host using the vCenter System account. Once the VM is created, data associated with the VM is automatically saved in the VM's assigned virtual disk. The vCenter System account can change the VM name or virtual disk name. The Administrator assigns the host IP address when expanding storage.

The storage policy contains the following defaults that can only be changed by the vCenter System role:

- Number of disk stripes per object: 1
- Flash read cache reservation: 0%
- Number of failures to tolerate: 1
- Force provisioning: No
- Object space reservation: 0%
- Disable object checksum: No
- IOPS: 0

- Failure tolerance method: RAID-1 (Mirroring) - Performance

The VxRail Manager GUI provides the Administrator with extension data on system health to include statistics and health on disks, nodes, power supplies, storage IOPS, CPU usage, and memory usage. The Administrator can also install VMs assigning a VM name, management IP address, and the time zone for the VM. The Administrator can also delete virtual disk files from the data store, and unregister VMs.

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

7.1.5 Protection of the TSF

Storage can be defined with different fault tolerance policies. The fault tolerance policy is set in vCenter and sent to ESXi for enforcement as part of a storage policy. The TOE is capable of preserving a secure state in case of a failure of a disk on a node, multiple disks on a node, or all disk on a node. The TOE uses vSAN mirroring to ensure that it maintains a secure state in the event of a node failure, or multiple disk failures on a single node. vSAN mirroring takes all data stored on one node, and creates a duplicate copy of that data onto another node. This prevents the loss of any data when any of these types of failures occur, which allows the TOE to remain fully operational and secure in the event of these failures.

ESXi sends availability of CPU, storage, and networks to vCenter to ensure it does not allocate unavailable resources. Storage policies and VM configurations are created and modified in the vCenter VM. These policies and configurations are sent to ESXi to enforce using a vCenter System role called *vpxuser.* This account is a system account that is only used between the vCenter VM and the ESXi hypervisor. The hypervisor receives updated policies and configurations and confirms resource availability before replacing the currently stored policies or configurations. The TOE applies the storage policies and VM configurations to all VMs installed on the VxRail appliance. The VMs installed on the VxRail appliance are the subjects of the quota. However, if the requested configurations are not available when verified for resource availability, the TOE does not apply these storage policies and VM configurations.

The TOE receives time from a networked NTP server. The host operating system uses the NTP provided time to provide a reliable timestamp for the TOE to use in auditing.

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

7.1.6 Resource Utilization

As described in Section 7.1.5, the TOE is designed to allow all disks on a node, multiple disks on a node, or one disk on a node to fail from disk read errors while maintaining stored data and the access control to that data.

The TSF enforces maximum quotas on the VMs. Each VM includes a .VMDK file, which is a file that stores all the VM's data. These VMDKs can have size restrictions placed on them so that they do not consume too much of the available resources. If a VM exceeds the defined size for their .VMDK file, it will not be allowed to perform anymore write operations. These restrictions are also part of a defined VM storage policy that is created in vCenter and sent to ESXi for enforcement.

TOE Security Functional Requirements Satisfied: FRU_FLT.2 and FRU_RSA.1.

7.1.7 TOE Access

All interfaces to the TOE allow the Administrator to log out and end the session. The VxRail Manager GUI has a **Signout** button that allows the Administrator to end their session. The Linux Shell Interface allows the Administrator to type `exit` to close the session on a terminal window, or select **Logout** button on IceWM, which presents a minimal graphical environment. Access to vSphere API is presented through the vSphere GUI of vCenter, which includes a **Logout** button that allows the Administrator to end their session. The VMware Host Client allows administrators to use the **Log out** button to end their session.

TOE Security Functional Requirements Satisfied: FTA_SSL.4

7.1.8 High Availability

The TOE monitors nodes for the percent of compute resources in use, SATA[16] DOM[17], and NIC status. These statistics are reported on the VxRail Manager GUI Logical Health page. The TOE uses its auto-discovery tools to determine node health. An Administrator can drill down into the diagram on the Physical Health page to pull additional information on the node. When the appliance is first setup and when any additional storage is added, the TOE performs a set of network tests to ensure the storage network is functioning properly. Removing a disk from the appliance without using the disk replacement workflow can result in damage to the disk and lost data. The VxRail Manager GUI detects the removal of a physical disk and displays an alert if a disk is removed without initiating the hardware removal process on the VxRail Manager GUI.

TOE Security Functional Requirements Satisfied: FHA_TST.1.

[16] SATA – Serial AT Attachment
[17] DOM – Disk on a Module

8. Rationale

8.1 Conformance Claims Rationale

This Security Target extends Part 2 and conforms to 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 16 below provides a mapping of the objectives to the threats they counter.

Table 16 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.AUDIT_COMPROMISE An attacker may cause audit records to be lost or modified or prevent future records from being recorded, thus masking an Administrator's actions.	O.AUDIT The TOE will provide the capability to detect security relevant events and create records of those events in the audit trail. These events must be protected from unauthorized modification and overwrite the oldest stored audit records once the log is full.	O.AUDIT mitigates this threat by ensuring that unauthorized attempts to access the TOE are recorded.
	O.TSF_PROTECT The TOE must protect its functions and TSF data to ensure its data and capabilities are intact when a disk read error causes a drive or node to fail. It also must provide the ability to check that its nodes, disks, and storage network are operating correctly.	O.TSF_PROTECT mitigates this threat by ensuring that TSF data, such as audit data, is protected by the TOE.
T.DATA_CORRUPTION An attacker may cause data to become corrupt or compromise TOE security due to hardware failure.	O.TSF_PROTECT The TOE must protect its functions and TSF data to ensure its data and capabilities are intact when a disk read error causes a drive or node to fail. It also must provide the ability to check that its nodes, disks, and storage network are operating correctly.	O.TSF_PROTECT mitigates this threat by providing mechanisms to protect the TSF data and disks from corruption.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT mitigates this threat by ensuring that the TOE is protected from external interference or tampering.

Threats	Objectives	Rationale
	O.USER_DATA_PROTECT The TOE must ensure the integrity of stored user data by monitoring for errors and automatically correcting the errors. The TOE must also ensure that denial of service will not occur because of unauthorized monopolization of resources.	O.USER_DATA_PROTECT mitigates this threat by monitoring user data for errors and rebuilding data if errors are found.
T.EXPLOIT An attacker may attempt to gain unauthorized access to the resources of the managed devices by exploiting vulnerabilities on a managed device.	O.ACCESS The TOE must enforce an access control policy in order to prevent unauthorized Users from gaining access to user data stored on the TOE. The TOE must also provide accessing Administrators with the ability to manage the TOE and its security attributes. Any Administrator accessing the TOE will be associated to a role.	O.ACCESS mitigates this threat by ensuring only authorized Users can obtain access to TOE storage.
	O.AUDIT The TOE will provide the capability to detect security relevant events and create records of those events in the audit trail. These events must be protected from unauthorized modification and overwrite the oldest stored audit records once the log is full.	O.AUDIT mitigates this threat by ensuring that security relevant events that may indicate attempts to tamper with the TOE are recorded.
	O.AUTHENTICATE The TOE must be able to identify and authenticate Administrators prior to allowing any access to TOE administrative functions and TSF data. The TOE must also provide mechanisms to visually protect passwords during authentication, verify that passwords meet the complexity requirements, and to end the current session while logged into the TOE.	O.AUTHENTICATE mitigates this threat by ensuring that all Administrators are authenticated and identified before allowing access to TOE.
	O.TSF_PROTECT The TOE must protect its functions and TSF data to ensure its data and capabilities are intact when a disk read error causes a drive or node to fail. It also must provide the ability to check that its nodes, disks, and storage network are operating correctly.	O.TSF_PROTECT mitigates this threat by ensuring continued operation of the TOE in a secure state in the event of disk failures.
T.UNAUTHORIZED _ACCESS An Administrator or User may gain unauthorized access (view, modify, or delete) to user data.	O.ACCESS The TOE must enforce an access control policy in order to prevent unauthorized Users from gaining access to user data stored on the TOE. The TOE must also provide accessing Administrators with the ability to manage the TOE and its security attributes. Any Administrator accessing the TOE will be associated to a role.	O.ACCESS mitigates this threat by ensuring that access to the data stored on the TOE is limited to Users with the appropriate access to the stored data.
	OE.AUTH The TOE environment must provide a secure repository of Administrator accounts used to manage the TOE.	OE.AUTH mitigates this threat by ensuring that the TOE environment provides a secure repository of Administrators authorized to manage the TOE.

Threats	Objectives	Rationale
	O.AUTHENTICATE The TOE must be able to identify and authenticate Administrators prior to allowing any access to TOE administrative functions and TSF data. The TOE must also provide mechanisms to visually protect passwords during authentication, verify that passwords meet the complexity requirements, and to end the current session while logged into the TOE.	O.AUTHENTICATE mitigates this threat by ensuring that Administrators are authenticated and identified prior to gaining access to TOE security data.
	O.TSF_PROTECT The TOE must protect its functions and TSF data to ensure its data and capabilities are intact when a disk read error causes a drive or node to fail. It also must provide the ability to check that its nodes, disks, and storage network are operating correctly.	O.TSF_PROTECT mitigates this threat by ensuring continued operation of the TOE in a secure state in the event of disk 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 17 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 17 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.ADMIN_AUTH The TOE environment provides a secure repository of Administrators that are authorized to manage the TOE.	OE.AUTH The TOE environment must provide a secure repository of Administrator accounts used to manage the TOE.	OE.AUTH upholds this assumption by ensuring that the vCenter virtual machine provides a repository of Administrators.
A.ADMIN_PROTECT The TOE environment provides the workstation used to manage the TOE that is free of malicious software.	OE.ADMIN_PROTECT The Administrator workstation must be protected from any external interference or tampering.	OE.ADMIN_PROTECT upholds this assumption by ensuring that the Administrator workstation is protected from external interference or tampering.
A.NETWORK The TOE environment provides the routers, switches, cabling, connectors, and firewalls required for its operation and to ensure the TOE is secured and protected from interference or tampering.	OE.NETWORK The routers, switches, cabling, connectors, and firewalls on which the TOE is attached must be properly implemented such that the TOE is secured and protected from interference or tampering.	OE.NETWORK upholds this assumption by ensuring that the TOE environment will provide the appropriate connectivity to allow the TOE to perform its function in a secure manner.

Assumptions	Objectives	Rationale
A.NOEVIL The Administrators who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	NOE.TRUSTED_ADMIN Administrators are trusted to follow and apply all administrative guidance in a trusted manner.	NOE.TRUSTED_ADMIN upholds this assumption by ensuring that the Administrators who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.PHYSICAL The TOE hardware, data it contains, firewalls, and 10 GbE switch are assumed to be located in a physically secure facility.	NOE.PHYSICAL A secure access facility must protect the physical security of the TOE, the data it contains, firewalls, 10GbE, and the TOE environment.	NOE.PHYSICAL upholds this assumption by ensuring that a secure access facility is used to physically security of the TOE, the data it contains, and the TOE environment.
	OE.NETWORK The routers, switches, cabling, connectors, and firewalls on which the TOE is attached must be properly implemented such that the TOE is secured and protected from interference or tampering.	OE.NETWORK upholds this assumption by ensuring that the TOE environment will provide the appropriate connectivity to allow the TOE to perform its function in a secure manner.
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.	OE.PROTECT satisfies the assumption that the TOE environment provides protection from external interference and 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 FHA requirements was created to specifically address the high availability self-tests performed by the TOE. The purpose of this family of requirements is to call out high availability functionality provided by the TOE. These requirements have no dependencies since the stated requirements embody all the necessary security functions. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended TOE security assurance requirements.

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

Table 18 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE must enforce an access control policy in order to prevent unauthorized Users from gaining access to user data stored on the TOE. The TOE must also provide accessing Administrators with the ability to manage the TOE and its security attributes. Any Administrator accessing the TOE will be associated to a role.	FDP_ACC.1 Subset access control	The requirement meets the objective by enforcing the Virtual Disk Access policy on all subjects and all named objects and all operations among them. The Virtual Disk Access policy specifies the access rules between all subjects and all named objects controlled by the TOE. While authorized Administrators are trusted to some extent, this requirement ensures only authorized access is allowed to named objects.
	FDP_ACF.1 Security attribute based access control	The requirement meets the objective by specifying the Virtual Disk Access policy rules that will be enforced by the TSF and determines if an operation among subjects and named objects is allowed. Furthermore, it specifies the rules to explicitly authorize or deny access to a named object based upon security attributes.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring Administrators with the ability to manage security attributes for the TOE.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by ensuring that the TOE provides restrictive default values for security attributes, and specifies alternative initial values to override the default values when an object or information is created.
	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 Administrators with roles to provide access to TSF management functions, security attributes, and TSF data.
O.AUDIT The TOE will provide the capability to detect security relevant events and create records of those events in the audit trail. These events must be protected from unauthorized	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_STG.1 Protected audit trail	The requirement meets the objective by ensuring that only authorized Administrators are able to modify and delete logs.

Objective	Requirements Addressing the Objective	Rationale
modification and overwrite the oldest stored audit records once the log is full.	FAU_STG.4 Prevention of audit data loss	The requirement meets the objective by preventing the loss of audit data by overwriting oldest log files if audit trail becomes full.
	FPT_STM.1 Reliable time stamps	This requirement meets the objective by providing reliable time stamps for audit records, preserving the order of events.
O.AUTHENTICATE The TOE must be able to identify and authenticate Administrators prior to allowing any access to TOE administrative functions and TSF data. The TOE must also provide mechanisms to visually protect passwords during authentication, verify that passwords meet the complexity requirements, and to end the current session while logged into the TOE.	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that every Administrator is authenticated before the TOE performs any TSF-mediated actions on behalf of that Administrator.
	FIA_UAU.7 Protected authentication feedback	The requirement meets the objective by ensuring that an attacker cannot read an Administrator's password during authentication because they are visually obscured.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that every Administrator is identified before the TOE performs any TSF-mediated actions on behalf of that Administrator.
	FTA_SSL.4 User-initiated termination	The requirement meets the objective by ensuring that Administrators have a method of closing their current session and keeping unauthorized Administrators from gaining control of an open session.
O.TSF_PROTECT The TOE must protect its functions and TSF data to ensure its data and capabilities are intact when a disk read error causes a drive or node to fail. It also must provide the ability to check that its nodes, disks, and storage network are operating correctly.	FPT_FLS.1 Failure with preservation of secure state	The requirement meets the objective by ensuring that the TOE preserves a secure state upon the detection of a disk read error that causes a disk or node failure.
	FPT_TDC.1 Inter-TSF basic TSF data consistency	The requirement meets the objective by ensuring that TSF data received from the vCenter server is consistently interpreted.
	FRU_FLT.2 Limited fault tolerance	The requirement meets the objective by ensuring the continued operation of the TOE in the event that a disk read error causes a drive or node to fail.
	FHA_TST.1 TSF health testing	The requirement meets the objective by ensuring that the TOE performs self-tests on node, disks, and storage network.
O.USER_DATA_PROTECT The TOE must ensure the integrity of stored user data by monitoring for errors and automatically correcting the errors. The TOE must also ensure that denial of service will not occur because of unauthorized monopolization of resources.	FDP_SDI.2 Stored data integrity	The requirement meets the objective by ensuring that the TOE monitors user data for integrity errors and corrects errors when possible.
	FRU_RSA.1 Maximum quotas	The requirement meets the objective by ensuring that the TSF assigns maximum quotas on subjects. This ensures that denial of service to subjects is not possible.

8.5.2 Security Assurance Requirements Rationale

EAL 2+ 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 System 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 EAL 2+, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 19 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 19 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.4	FAU_STG.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FMT_MSA.3	✓	
	FDP_ACC.1	✓	
FDP_SDI.2	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.7	FIA_UAU.1	✓	Although FIA_UUA.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	✓	
FMT_MSA.1	FMT_SMR.1	✓	
	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3	FMT_SMR.1	✓	
	FMT_MSA.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FPT_FLS.1	No dependencies	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FPT_STM.1	No dependencies	✓	
FPT_TDC.1	No dependencies	✓	
FRU_FLT.2	FPT_FLS.1	✓	
FRU_RSA.1	No dependencies	✓	
FTA_SSL.4	No dependencies	✓	
FHA_TST.1	No dependencies	✓	

9. Acronyms

Table 20 defines the acronyms used throughout this document.

Table 20 – Acronyms

Acronym	Definition
API	Application Programming Interface
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
CPU	Central Processing Unit
DNS	Domain Name Service
DOM	Disk on a Module
EAL	Evaluation Assurance Level
GbE	Gigabit Ethernet
GUI	Graphical User Interface
HDD	Hard Disk Drive
ID	Identification
IOPS	Input/Output Operations per Second
IP	Internet Protocol
IT	Information Technology
Mbps	Megabits per second
NIC	Network Interface Cards
OS	Operating System
PP	Protection Profile
PSC	Platform Services Controller
QoS	Quality of Service
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
REST	Representational State Transfer
SAN	Storage Attached Network
SAR	Security Assurance Requirement
SATA	Serial AT Attachment
SDDC	Software-Defined Data Center
SFP+	Enhanced Small Form-factor Pluggable

Acronym	Definition
SFR	Security Functional Requirement
SSD	Solid State Drives
SSO	Single Sign-On
ST	Security Target
TB	Terabyte
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
2U	Two rack Units
UI	User Interface
VM	Virtual Machine
vSAN	Virtual Storage Attached 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