CyberArk Software, Ltd.

Privileged Account Security Solution v9.1

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.8

Prepared for:

CYBERARK®

CyberArk Software, Ltd.
57 Wells Avenue, Suite 20A
Newton, MA 02459
United States of America

Phone: +1 (888) 808-9005
Email: info@cyberark.com
http://www.cyberark.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
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the organization of the ST. The TOE is the CyberArk Privileged Account Security Solution v9.1, and will hereafter be referred to as the TOE throughout this document.

The TOE is software-based solution for Privileged Account Security management in the enterprise. The Privileged Account Security (PAS) Solution enables organizations to secure, provision, control, and monitor all activities associated with privileged identities used in enterprise systems and applications.

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 functions 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 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 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	CyberArk Software, Ltd. Privileged Account Security Solution v9.1 Security Target
ST Version	Version 1.8
ST Author	Corsec Security, Inc.
ST Publication Date	2015-04-24

ST Title	CyberArk Software, Ltd. Privileged Account Security Solution v9.1 Security Target
TOE Reference	CyberArk Software, Ltd. Privileged Account Security Solution v9.1 • Enterprise Password Vault v9.1; Build 9.10.0.141 • Password Vault Web Access v9.1; Build 9.10.0.275 • PrivateArk Client v8; Build 8.00.4.10 • Privileged Session Manager v9.1; Build 9.10.0.30 • Privileged Session Manager SSH Proxy v7.2.14; Build 7.20.140.29 • Central Policy Manager v9.1; Build 9.10.0.98 • On-Demand Privileges Manager v7.2.11; Build 7.20.110.8 • Application Identity Manager v7.2.13; Build 7.2.130.10
FIPS[1] 140-2 Status	FIPS 140-2 Validation Certificate #: 1747 and 1051

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.

CyberArk's PAS Solution v9.1 is a full, software-based solution for managing the most privileged accounts in the enterprise. The solution enables organizations to secure, provision, control, and monitor all activities associated with enterprise systems and applications. At the heart of the PAS Solution lies a Patented Digital Vault™ which is designed to meet the highest security requirements. The Digital Vault, also known as the Enterprise Password Vault (EPV), provides numerous security capabilities for authentication, encryption, tamper-proof audit, and data protection. The EPV provides secure storage and sharing of privileged account credentials, audit data, and recorded privileged account sessions, using multiple layers of encryption and security.

The EPV is run on a dedicated server and is protected by the Windows firewall, which only allows communication to and from the vault via CyberArk's proprietary communications channel. Access to the PAS Solution can be controlled by one or more authentication methods including: LDAP[2] authentication, PKI[3] digital certificates, RSA[4] SecurID tokens, two-way authentication, RADIUS[5], USB[6] tokens, and Windows Authentication. Once logged in, users will only see the privileged accounts they have permission to see, completely unaware of other privileged accounts.

The EPV uses multiple layers of encryption to provide maximum security of the contents of each safe. Each data[7] file within a safe is encrypted with a unique file encryption key. Those file encryption keys are stored within the safe and encrypted with a safe encryption key unique to the safe. The safe encryption keys stored within the vault are encrypted with a unique vault encryption key. All of these keys are only delivered to those users with appropriate access control rights. Administrators can define access to safes and data within the safes so that users must be manually confirmed by a Safe Supervisor before they can access the safe and its contents.

[1] FIPS – Federal Information Processing Standards
[2] LDAP – Lightweight Directory Access Protocol
[3] PKI – Public Key Infrastructure
[4] RSA – Rivest, Shamir, Adleman
[5] RADIUS – Remote Authentication Dial In User Server
[6] USB – Universal Serial Bus
[7] The term "data" constitutes all privileged user accounts, audit data, recorded sessions, and miscellaneous files

The Privileged Account Security Solution is comprised of multiple, standalone CyberArk products which help to protect, manage, and audit user and application credentials and monitor all privileged activity. Each product works together to provide a complete, secure solution to solve the different requirements for privileged account security. The PAS Solution is a plug-and-play, ready-to-use solution that implements its security features immediately after component installation. The following sections describe each of the products which make up the Privileged Account Security Solution.

1.3.1 Privileged Account Security Solution Components

The Privileged Account Security Solution provides a secure environment within an enterprise where all administrative passwords can be securely archived, transferred, and shared by authorized users (such as IT[8] Staff, on-call administrators, and local administrators in remote locations). Access to and management of the PAS Solution is provided by a Windows client, a Web interface, and a variety of other APIs[9]. Each component of the PAS Solution solves the different requirements for privileged account security.

1.3.1.1 Enterprise Password Vault (EPV)

The EPV is deployed on a dedicated standalone server running a hardened version of Microsoft Windows Server. This ensures the most isolated and secure storage possible for EPV contents. The EPV may be deployed as a high-availability cluster, where the standby EPV will immediately take over if the production EPV fails to process requests. A Disaster Recovery instance of the EPV may also be used to replicate EPV data and immediately fail-over if the production EPV instances stop processing requests.

The Digital Vault secures privileged credentials based on the privileged account security policy, or Master Policy™, and controls who can access which passwords and when. The Master Policy Engine enables administrators to set, manage, and monitor a single privileged account security policy. This enables fast implementation and flexibility to set an enterprise-wide policy.

The EPV is designed to continually discover changes to the IT environment with its Discovery Engine. As new servers and workstations are added or removed, changes in the privileged accounts are automatically discovered and updated. The EPV is accessed and managed through the various Client interfaces. These interfaces include a Windows client-based interface (known as the PrivateArk Client) as well as a web-based Graphical User Interface (GUI) (known as the PrivateArk Web Client).

1.3.1.2 Password Vault Web Access (PVWA) Interface

The Password Vault Web Access Interface is a fully-featured web interface that provides a single console for requesting, accessing, and managing privileged account credentials passed throughout the enterprise by both end-users and administrators. The PVWA dashboard enables users to see an overview of activities in the PAS Solution, as well as statistics about all the activities that have taken place.

1.3.1.3 PrivateArk Client

The PrivateArk Client is a regular Windows application that is used as the administrative client for the PAS Solution. The Client can be installed on multiple remote computers and can access the EPV via LAN[10], WAN[11], or through the Internet via the Web version of the client. From this interface, users can define a vault hierarchy and create safes and users. Access to the EPV via the PrivateArk Client requires a user to be authenticated by the Digital Vault.

1.3.1.4 Privileged Session Manager (PSM)

The Privileged Session Manager enables an organization to secure, control, and monitor privileged access to a network device. The PSM acts as a gateway to facilitate the communication with remote devices. The

[8] IT – Information Technology
[9] API – Application Programming Interface
[10] LAN – Local Area Network
[11] WAN – Wide Area Network

PSM controls user access to privileged accounts and automatically initiates privileged sessions to third-party devices over a variety of connection protocols such as RDP[12]. The PSM separates the end-users from targets, enabling connections to privileged devices without having to divulge the passwords to the end-user.

The PSM can record all activities that occur in a privileged session and can provide a playback of each recorded session to authorized auditors. Recorded sessions are securely stored and protected in the EPV. The PSM is integrated transparently and seamlessly into existing enterprise infrastructures.

1.3.1.5 Privileged Session Manager SSH Proxy (PSMP)

The PSMP is a Linux-based application similar to the PSM, but acts as a proxy for SSH[13]-enabled devices. PSMP controls access to privileged sessions and initiates SSH connections to remote devices on behalf of the user without the need to disclose SSH credentials. PSMP records text-based sessions which are stored in the EPV, later to be viewed by an authorized auditor. Unique to the PSMP are the Single Sign-On capabilities, which allow users to connect to target devices without being exposed to the privileged connection password.

1.3.1.6 Central Policy Manager (CPM)

The Central Policy Manager automatically enforces enterprise security policy by automatically changing passwords on remote machines and storing the new passwords in the EPV, all without any human interaction. The CPM is capable of generating new random passwords and replacing existing passwords on remote machines, and saving the new passwords in the EPV. Passwords monitored and generated by the CPM conform to the Master Policy created by the enterprise. Administrators will be notified via the PVWA when passwords are about to expire, are expired, or do not meet the Master Policy criteria. Administrators can also implement a one-time password policy, which requires a password to be changed each time a user logs in with the existing password.

1.3.1.7 On-Demand Privileges Manager (OPM)

The On-Demand Privileges Manager enables organizations to secure, control, and monitor access to privileged UNIX/Linux commands. Users can perform super-user tasks with their own personal account, all while maintaining the least-privilege concept.

1.3.1.8 Application Identity Manager (AIM)

The Application Identity Manager is a Windows- and Linux- based application that facilitates access to privileged passwords and eliminates the need to hard-code plaintext passwords in applications, scripts, or configuration files. As with all other credentials stored in the EPV, AIM passwords are stored, logged, and managed securely. AIM is separated into two components: a Provider, which securely retrieves and caches passwords and provides immediate access to the calling application; and the SDK, which provides a set of APIs for Java, .NET, COM[14], CLI[15], and C/C++. In the evaluated configuration, the AIM Provider for Windows and SDK are excluded.

1.3.1.9 PrivateArk Vault Command Line Interface (PACLI)

The PACLI enables users to access the PAS Solution from any location using automated scripts, in a command line environment. Users accessing the PAS solution via the PACLI have access to a limited interface for management, control, and audit features. The PACLI is not included in the evaluated configuration of the TOE.

[12] RDP – Remote Desktop Protocol
[13] SSH – Secure Shell
[14] COM – Component Object Model
[15] CLI – Command Line Interface

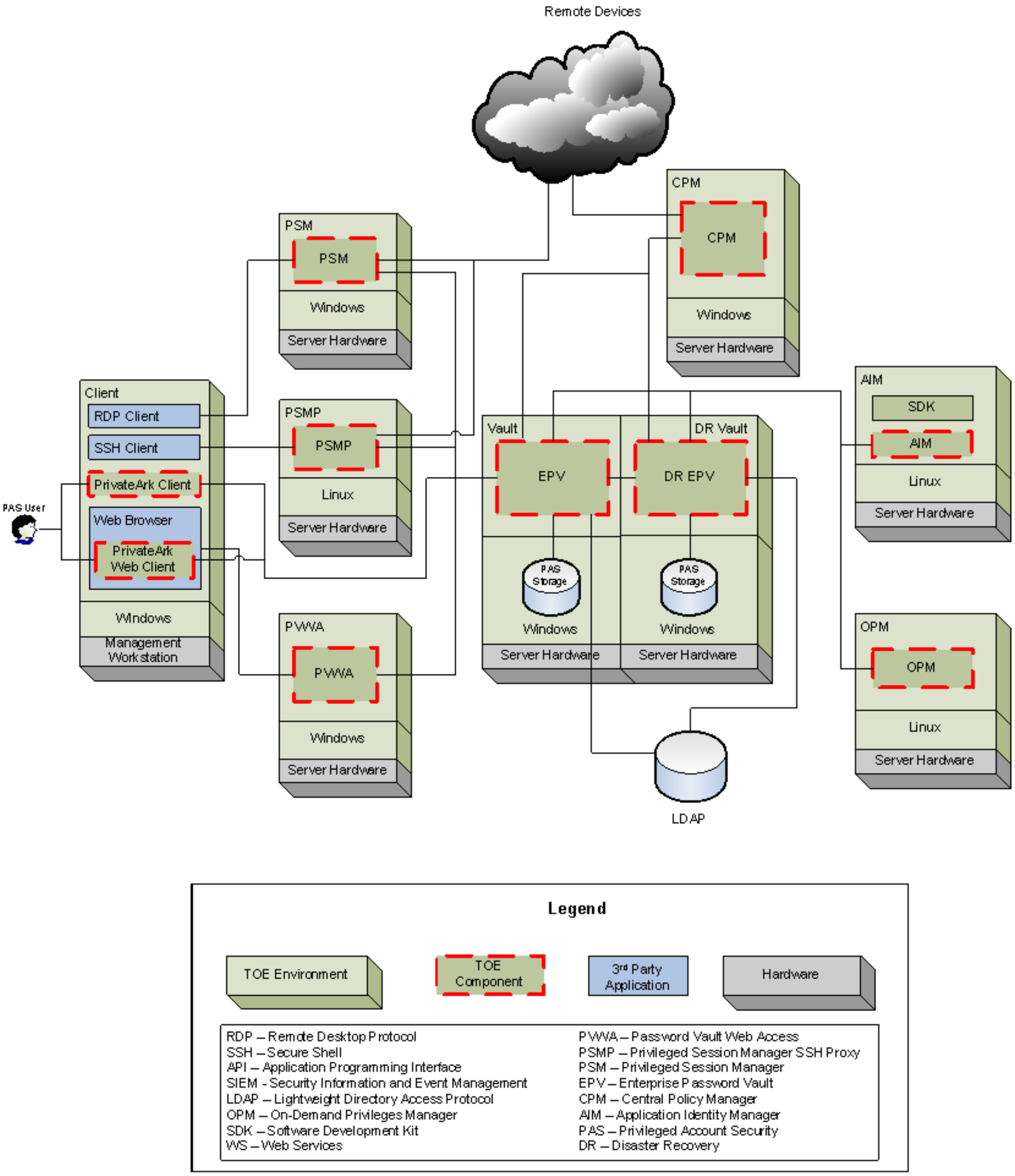
1.4 TOE Overview

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

The TOE is software-based identity management solution for managing privileged accounts in the enterprise. The PAS Solution v9.1 is comprised of multiple standalone software and interfaces modules which enable organizations to secure, provision, control, and monitor all activities associated with enterprise systems and applications. The software components of which the TOE is comprised of are:

- Enterprise Password Vault
- PrivateArk Client
- Privileged Session Manager
- Privileged Session Manager SSH Proxy
- Central Policy Manager
- On-Demand Privileges Manager
- Application Identity Manager
- Password Vault Web Access

Each component of the TOE and its functionality is described in Section 1.3 (Product Overview) above. TOE components and the TOE boundary are represented in Figure 1 below.



RDP – Remote Desktop Protocol
SSH – Secure Shell
API – Application Programming Interface
SIEM - Security Information and Event Management
LDAP – Lightweight Directory Access Protocol
OPM – On-Demand Privileges Manager
SDK – Software Development Kit
WS – Web Services
PVWA – Password Vault Web Access
PSMP – Privileged Session Manager SSH Proxy
PSM – Privileged Session Manager
EPV – Enterprise Password Vault
CPM – Central Policy Manager
AIM – Application Identity Manager
PAS – Privileged Account Security
DR – Disaster Recovery

Figure 1 TOE Boundary

The TOE includes all of the components and functionality described above and in section 1.3.1. The features and functionality listed below in Section 1.4.1 are not included in the TOE, but are vital for the complete functionality of the TOE. Section 1.4.1 identifies any major non-TOE hardware and software that is required by the TOE including the TOE minimum requirements.

1.4.1 TOE Environment

The Enterprise Password Vault is installed on a hardened[16] version of Microsoft Windows Server. Access to and from the Windows server is available to only components of the Privileged Account Security Solution via a proprietary access protocol. Local storage for the password vault is provided by the Windows Server host device hardware. EPV contains its own LDAP client and can access a local LDAP server, which is used for TOE user authentication.

Access to the PrivateArk Web Client as well as access to the Password Vault Web Access requires the TOE user to have access to the Internet and a compatible web browser. Compatible web browsers that can be used to access these components are listed in Table 2 below. Access to the PrivateArk Web Client and PVWA also requires that they be installed on a machine with access to the network.

A TOE user can access the PSM through a remote desktop client such as Windows Remote Desktop Connection. The client must implement the RDP protocol. Access to the PSMP can be obtained by a TOE user either directly accessing the Linux Shell system or through a third-party Windows Shell application, such as Putty.

All other components of the TOE must be installed onto hardware devices running either a Windows or Red Hat Enterprise Linux Operating System (OS). All TOE components require access to the same network in which the EPV was installed order to interact with it. Remote devices wishing to use the PSM, PSMP, or CPM also require access to the network through a secure VPN[17] session.

It is assumed that there will be no untrusted users or software on the TOE Server components. Access to the TOE environment OS's must be limited to authorized users and secured with an authentication method. In addition, the TOE Server components are intended to be deployed in a physically secured cabinet, room, or data center with the appropriate level of physical access control and physical protection (e.g. badge access, fire control, locks, alarms, etc.).

Table 2 defines the minimum system requirements and supported platforms for installing and accessing the PAS Solution v9.1.

Table 2 TOE Minimum Requirements

Requirement
TOE Hardware Requirements (for all TOE components): • Quad Core Processor (Intel) • 8 GB[18] RAM[19] • 2x 80 GB SATA[20]/SAS[21] hot-swappable drives • RAID[22] Controller • 1Gb[23] Network Adapter

[16] Protected by a firewall which only allows remote communications from CyberArk applications via their proprietary communications protocol.
[17] VPN – Virtual Private Network
[18] GB – Gigabyte
[19] RAM – Random Access Memory
[20] SATA – Serial Advanced Technology Attachment
[21] SAS – Serially Attached SCSI (Small Computer System Interface)
[22] RAID – Redundant Array of Independent Disks
[23] Gb – Gigabit

Requirement
TOE Operating System Requirements: • Windows 2012 R2 - Hardened ○ EPV • Windows 2012 R2 (64-bit) ○ PSM ○ PVWA ○ CPM • Red Had Enterprise Linux (RHEL) 5.3 (64-bit) ○ AIM ○ OPM ○ PSMP
Operating System (PrivateArk Client): Windows 7 Enterprise SP1 (32 or 64-bit)
LDAP Directory: MS[24] Active Directory
Browser: Microsoft Internet Explorer 10.0
Prerequisites: • .NET Framework 3.5 SP1 • Microsoft IIS[25] 7.5 or later • RDP ActiveX Client 5.2 or higher • Java Runtime Environment (JRE) 1.4 or higher • Adobe Flash Player 10.0 or higher • Remote Desktop Services (RDS) Session Host

In the evaluated configuration, the EPV, PSM, PVWA, and CPM components are installed on Windows Server 2012 R2. The AIM, OPM, and PSMP components are installed on Red Hat Enterprise Linux 5.3. The PrivateArk Client is installed on Windows 7 Enterprise. The web browser used to access the PVWA is Internet Explorer 10.0. The authentication server used is Windows 2012 R2 Active Directory Domain Services.

1.5 TOE Description

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

1.5.1 Physical Scope

Figure 1 in Section 1.4 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

The TOE is a software-only Privileged Account Security solution that runs on both Windows and Linux operating Systems. The Windows and Linux Operating Systems can be installed on any server hardware that meets the hardware criteria listed in Table 2 above. The EPV must be installed on its own, separate Windows server device. Each of the other TOE components are standalone software components and may be in installed onto the same sever appliance or separate server appliances. The servers must have access to the same network on which the EPV is installed.

The TOE Boundary includes all the CyberArk developed parts of the Privileged Account Security Solution v9.1 product. Any third-party source code or software that PAS Solution v9.1 has modified is considered

[24] MS – Microsoft Services

[25] IIS – Internet Information Services

to be TOE Software. The TOE Boundary specifically does not include any of the third party software that the TOE relies upon as described in Section 1.4.1. The TOE Boundary also does not include the third-party LDAP server, which stores authentication data for the TOE.

1.5.1.1 Guidance Documentation

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

- Privileged Account Security Installation Guide
- Privileged Account Security End User Guide
- Privileged Account Security Implementation Guide
- Privileged Account Security Reference Guide
- Privileged Account Security System Requirements
- Privileged Account Security Release Notes
- Application Identity Management Implementation Guide

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
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF[26]
- Resource Utilization
- TOE Access
- Trusted Path/Channel

1.5.2.1 Security Audit

The Security Audit function provides the TOE with the functionality of generating audit records. Typical audit records that can be accessed by a user with the correct authorizations include Privileged Account Inventory, Safe Lists, User Lists, and User Activities. As TOE users access, manage, and configure the TOE, their activities are tracked. When an Auditor user (TOE user with the “View audit” authorization) generates an “Activity Log”, it will be saved locally. The Auditor will see the various activities performed by TOE users in an organized list. Once an Activity Log has been generated, the results can be filtered with general filters, filters by target system, activities, and history of the activity. Only users with the correct authorizations and permission are capable of accessing the contents of the safe. Unauthorized access, deletion, and modification of the records is not possible.

1.5.2.2 Cryptographic Support

The TOE implements FIPS 140-2 Approved cryptographic algorithms to support cryptographic activities such as encryption, decryption, and hashing. The cryptographic module within the TOE generates a unique AES[27] 256-bit key for each individual safe located in the EPV. Additionally, each account and file located within each safe is protected by a unique AES 256-bit key. AES, RSA, and HMAC[28] are all used by the TOE when performing a TLS or SSH session with a remote machine. All AES, RSA, and HMAC keys are generated with an SP 800-90 DRBG[29], or in some cases, ANSI[30] X9.31.

[26] TSF – TOE Security Functionality
[27] AES – Advanced Encryption Standard
[28] HMAC – (keyed-) Hash Message Authentication Code
[29] DRBG – Deterministic Random Bit Generator

Each of the cryptographic algorithms supported by the TOE have been tested and certified by the CAVP[31]. Each algorithm has been awarded a certificate number. The TOE performs FIPS 140-2 Approved methods for encryption, decryption, hashing, random number generation, and key transport. The TOE is responsible for destroying all ephemeral keying material generated within the TOE boundary.

1.5.2.3 User Data Protection

The TOE enforces two access control policies which limit access to the safes located on the EPV (Vault Access Control Policy) and further limit access to the accounts and files stored within the safes (Safe Access Control Policy). Access to the vault and safes are enforced by user account authorizations and permissions. Once granted access to the EPV, the users with the correct authorizations can manage the vault and the safes within the vault. This includes the creation of safes and the management of file types allowed within each safe.

In order for a user to access the contents within a safe, they must be added as a safe member by a safe member with the "Manage Safe Members" permission. Each safe member is given safe permissions which allow them to read, write, and remove accounts and files located within the safe.

1.5.2.4 Identification and Authentication

TOE users must provide the correct username and password associated an external LDAP account. The TOE must successfully identify users prior to allowing any actions on their behalf. The TOE identifies the user by passing the username and password combination to the LDAP server for validation.

1.5.2.5 Security Management

Management of the TOE can be defined as "granular". Each TOE user that is granted access to the TOE is provided with a profile which defines the user's access rights, management rights, and action rights within the TOE. When first creating a user in the vault and when providing them access to a safe, the TOE enforces restrictive default values by not providing the user with any authorizations or permissions. Security roles can also be defined for a TOE user based on a collection of vault authorizations and safe permissions given to the user.

1.5.2.6 Protection of the TSF

The TOE employs a multi-layered encryption scheme in order to protect the credentials stored within the EPV. The three layers of encryption employed by the EPV are the vault layer, safe layer, and account/file layer. All accounts, files, safes, and even the vault itself are encrypted with unique encryption keys.

The PAS Solution v9.1 components all communicate with one another through CyberArk's patented communications protocol, which employs AES-256 for confidentiality and HMAC SHA-1 for integrity.
The TOE provides seamless switching between the main EPV and a back-up (Disaster Recovery) Vault if a failure to the main EPV occurs.

1.5.2.7 Resource Utilization

The TOE provides seamless switching between the main EPV and a back-up (Disaster Recovery) Vault if a failure to the main EPV occurs. Types of failures include physical and logical destruction of the EPV (or its host server) or loss of network connectivity. This transparent failover ensures that regular access to the TOE and its functions is maintained.

1.5.2.8 TOE Access

TOE users attempting to access the TOE through the PVWA or PrivateArk client will encounter a display banner prior to being able to log into the TOE. The banner provides access to an advisory warning

[30] ANSI – American National Standards Institute

[31] CAVP – Cryptographic Algorithm Validation Program.

message regarding the unauthorized use of the TOE. Access to the TOE will be limited to users that provide the correct username and password combination. Restrictions can be placed on a TOE user which will deny them access to the TOE. Users must actively interact with the TOE in order to avoid session termination. If the user has not interacted with the TOE for 10 minutes via the PVWA, or for an administrator-defined inactivity period (default of 30 minutes) via the PrivateArk Client, the session will terminate and the user will be logged out of the TOE.

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

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

- Supported Windows Operating Systems other than those listed in Table 2
- CyberArk Events Notification Manager
- AIM Provider for Windows
- AIM SDK[32]
- Web Services (WS) API
- PACLI
- CyberArk Remote Control
- Multiple PSM Implementations
- Multiple CPM Implementations
- Mobile PVWA
- Local user authentication
- NT/Windows Authentication
- RADIUS Authentication
- RSA SecurID Authentication (in PVWA)
- PKI Authentication (Personal Certificate)
- Oracle SSO[33] (in PVWA)
- High Availability mode

[32] SDK – Software Development Kit

[33] SSO – Single Sign-On

2 Conformance Claims

Table 3 provides 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, Revision 4, September 2012; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2014/05/02 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[34] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into four categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)
- TOE failure: The threat of the TOE failing in its operations or exhausting its resources which leads to a failure of TOE operations.
- External IT Entities: External IT entities that are being used by malicious attackers to adversely affect the security of the TOE.

Both 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. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. The threats listed in Table 4 are applicable.

Table 4 Threats

Name	Description
T.ADMIN_ERROR	An administrator may incorrectly configure the TOE resulting in ineffective security mechanisms.
T.AUDIT_COMPROMISE	A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future records from being recorded, thus masking a user's actions.
T.DATA_COMPROMISE	An unauthorized user may read, modify, delay, or destroy security critical TOE data stored on the TOE or being transmitted between physically separated parts of the TOE.
T.MASQUERADE	A malicious user, process, or external IT entity may masquerade as an authorized entity to gain unauthorized access to data or TOE resources.
T.UNAUTHORIZED _ACCESS	A user may gain unauthorized access (view, modify, delete) to user

[34] IT – Information Technology

[35] TSF – TOE Security Functionality

Name	Description
	data.
T.UNIDENTIFIED _ACTIONS	The administrator may fail to notice potential security violations, thus preventing the administrator from taking action against a possible security violation.
T.DISASTER	Operation or access to the TOE may suddenly fail, rendering the TOE useless

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 defined for this ST.

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.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.
A.TRUSTED_ADMIN	TOE Administrators are non-hostile and are trusted to follow and apply all administrator guidance.
A.HARDEN	The EPV component of the TOE will be installed on a hardened instance of Windows
A.ACCESS	Access to the TOE will be provided by a reliable network connection
A.INSTALL	TOE components will be installed onto a compatible Operating System
A.INTERNAL_SERVICES	All LDAP and remote systems that the TOE communicates with should be located on the same internal network as the TOE. Users on this network are assumed to be non-hostile.

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.

Table 6 Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE will ensure that only authorized users may gain access to it and the resources that it controls.
O.AUDIT	The TOE will provide the capability to detect security relevant events and record them to the audit trail.
O.AUDIT_REVIEW	The TOE will provide the capability for only authorized users to view audit information.
O.AUDIT_STORAGE	The TOE will provide a secure method of storing local audit records.
O.CRYPTO	The TOE will provide FIPS 140-2 Approved cryptographic algorithms and procedures to TOE users during operation of the TOE.
O.USER_AUTHEN	The TOE will uniquely identify and authenticate users prior to allowing access to TOE functions and data.
O.PROTECT_COMM	The TOE will provide protected communication channels for parts of the distributed TOE.
O.BANNER	The TOE will present an access banner to TOE users prior to accessing the TOE that defines acceptable use of the TOE
O.TOE_ADMIN	The TOE will provide mechanisms to ensure that only authorized administrators are able to configure the TOE security functions attributes.
O.ROBUST_ACCESS	The TOE will implement mechanisms that can deny or suspend session establishment
O.FAIL_SECURE	The TOE will provide a method to continue secure operations during a catastrophic TOE failure
O.VAULT	The TOE will provide mechanisms to ensure that stored credentials are not stored in plaintext and are protected from unauthorized access
O.PERMISSIONS	The TOE will provide a method to separate and restrict the abilities of individual TOE users

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The IT security objectives listed in Table 7 are to be satisfied by the environment:

Table 7 IT Security Objectives

Name	Description
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.
OE.HARDENED	The TOE environment must provide a hardened version of Windows for the installation of EPV.
OE.NETWORK	The TOE environment must provide a consistent network connection to the TOE.
OE.OS	The TOE environment must provide a compatible Windows or Linux Operating System version for the installation of TOE components.
OE.TRUSTED_ADMIN	Trusted TOE Administrators must follow and apply all administrator and configuration guidance.
OE.INTERNAL_SERVICES	LDAP servers and remote systems accessed by the TOE are located on the same internal network as the TOE. Users on this network are non-hostile.

4.2.2 Non-IT Security Objectives

The non-IT environment security objectives listed in Table 8 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	The TOE environment must provide physical security commensurate with the value of the TOE and the data it contains.

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.

5.1.1 Class FPT: Protection of the TSF

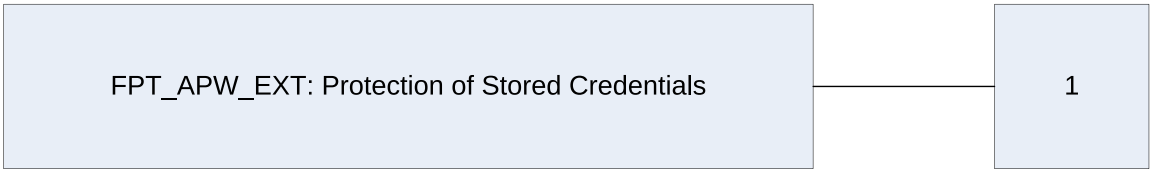
This class contains families of functional requirements that relate to the integrity and management of the mechanisms that constitute the TSF and to the integrity of TSF data.

5.1.1.1 FPT_APW_EXT Protection of Stored Credentials

Family Behavior

The requirements of this family ensure that the TSF will protect credential data from disclosure. This family is not modeled after any families in Common Criteria Part 2. There is only one component in this family, FPT_APW_EXT.1. This component requires the TOE to store credentials in non-plaintext form and to prevent the reading of plaintext credentials.

Component Leveling



FPT_APW_EXT.1 Extended: This SFR describes the behavior of the TOE when it must store credentials – either credentials for administrative users or credentials for enterprise users. An explicit requirement was required as there is no equivalent requirement in the Common Criteria. This SFR is defined in the Standard Protection Profile for Enterprise Security Management Identity and Credential Management. The SFR was further modified from the Protection Profile to reflect the functionality of the TOE.

Management: FPT_APW_EXT.1

a) There are no management activities foreseen.

Audit: FPT_APW_EXT.1

a) There are no audit activities foreseen.

FPT_APW_EXT.1 Protection of Stored Credentials
Hierarchical to: No other components.
Dependencies: No other components.
FPT_APW_EXT.1.1
The TSF shall store credentials in non-plaintext form
FPT_APW_EXT.1.2
The TSF shall prevent the reading of plaintext credentials from unauthorized users.

5.2 Extended TOE Security Assurance Components

There are no extended TOE Security Assurance Components.

6 Security Requirements

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

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets]. In keeping with these conventions, in the event an assignment is within a selection, it will be depicted as *italicized, underlined* text.
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "_EXT" at the end of the short name.
- Iterations are identified by appending a number in parentheses following the component title. For example, FDP_ACC.1(1) Audit Data Generation would be the first iteration and FDP_ACC.1(2) 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_SAR.2	Restricted audit review				
FAU_SAR.3	Selectable Audit Review		✓		
FAU_STG.1	Protected Audit Storage	✓			
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓	✓	
FDP_ACC.1(1)	Subset access control (Vault)		✓		✓
FDP_ACC.1(2)	Subset Access Control (Safe)		✓		✓
FDP_ACF.1(1)	Security attribute based access control (Vault)		✓		✓

Name	Description	S	A	R	I
FDP_ACF.1(2)	Security attribute based access control (Safe)		✓		✓
FIA_UAU.2	User authentication before any action				
FIA_UID.2	User identification before any action				
FMT_MOF.1(1)	Management of security function behavior (Vault)	✓	✓		✓
FMT_MOF.1(2)	Management of security function behavior (Safe)	✓	✓		✓
FMT_MSA.1(1)	Management of security attributes (Vault)	✓	✓		✓
FMT_MSA.1(2)	Management of security attributes (Safe)	✓	✓		✓
FMT_MSA.3(1)	Static attribute initialization (Vault)	✓	✓	✓	✓
FMT_MSA.3(2)	Static attribute initialization (Safe)	✓	✓	✓	✓
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_APW_EXT.1	Protection of Stored Credential				
FPT_FLS.1	Failure with preservation of secure state		✓		
FPT_ITT.1	Basic Internal TSF Data Transfer Protection	✓			
FRU_FLT.1	Degraded Fault Tolerance		✓		
FTA_SSL.3	TSF-Initiated Termination		✓		
FTA_TAB.1	Default TOE Access Banner				
FTA_TSE.1	TOE Sessions Establishment		✓		

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) [*Privileged account access, approval workflow, privileged account management, privileged account auto-detection, safe management, member management, user login, user/group/location management, Vault system administration, reports management, file access, file management*].

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, [*safe, target system, reason, alert*].

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

FAU_GEN.2 User identity association
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification
FAU_GEN.2.1

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

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

The TSF shall provide [*users with the "View audit" safe authorization*] with the capability to read [*operational reports and audit/compliance reports*] from the audit records.

FAU_SAR.1.2

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

FAU_SAR.2 Restricted audit review
Hierarchical to: No other components.
Dependencies: FAU_SAR.1 Audit review
FAU_SAR.2.1

The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 Selectable audit review
Hierarchical to: No other components.
Dependencies: FAU_SAR.1 Audit review
FAU_SAR.3.1

The TSF shall provide the ability to apply [*filters*] of audit data based on [*general filters, target systems, activities, and history*].

FAU_STG.1 Protected Audit Storage

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

FAU_STG1.1

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

FAU_STG1.2

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

6.2.3 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.
Dependencies: FCS_COP.1 Cryptographic operation
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*Hash DRBG, HMAC DRBG, CTR DRBG*] and specified cryptographic key sizes [*256-bit (AES), 2048-bit (RSA), 160-bit (SHA-1), and 128-bit (HMAC)*] that meet the following: [*SP 800-90*].

FCS_CKM.4 Cryptographic key destruction
Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2 zeroization requirements*].

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1

The TSF shall perform [*the operations listed in Table 10 below*] in accordance with a specified cryptographic algorithm [*algorithms listed in Table 10 below*] and cryptographic key sizes [*key sizes listed in Table 10 below*] that meet the following: [*standards listed in* Table 10 *below*]

Table 10 Cryptographic Algorithms

Cryptographic Operation	Cryptographic Operation	Key/Digest Size	Standard	Certificate Number
Symmetric encryption/decryption	*AES-CBC*	*256-bit*	*FIPS PUB 197*	695, 1884, 2116, 2234, 2342, 2394, 2484, 2824, 2929
Asymmetric encryption/decryption	*RSA 2048-bit*	*2048-bit*	*PKCS[36] #1 v1.5*	323, 960, 1086, 1145, 1205, 1273, 1477, 1535

[36] PKCS – Public Key Cryptography Standards

Cryptographic Operation	Cryptographic Operation	Key/Digest Size	Standard	Certificate Number
Hashing	*SHA-1*	*160-bit*	*FIPS PUB 180-4*	723, 1655, 1840, 1923, 2019, 2056, 2102, 2368, 2465
Message authentication	*HMAC SHA-1*	*160-bit*	*FIPS PUB 198-1*	373, 1126, 1288, 1363, 1451, 1485, 1526, 1768, 1856
Random number generation	*Hash DRBG,* *HMAC DRBG,* *CTR DRBG (AES)*	*N/A*	*NIST SP 800-90*	157, 229, 264, 292, 316, 342, 485, 540
	ANSI X9.31 (AES)	*128-bit,* *192-bit,* *256-bit*	*ANSI X9.31*	407

6.2.4 Class FDP: User Data Protection

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

FDP_ACC.1(1).1

The TSF shall enforce the [*Vault Access Control Policy*] on [

- *Subjects: users accessing EPV*
- *Objects: safes*
- *Operations: view, create*].

FDP_ACC.1(2) Subset access control (Safe)
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1(2).1

The TSF shall enforce the [*Safe Access Control Policy*] on [

- *Subjects: users accessing an EPV-hosted safe (safe members)*
- *Objects: accounts/passwords, files*
- *Operations: read, write, and remove*].

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

FDP_ACF.1(1).1

The TSF shall enforce the [*Vault Access Control Policy*] to objects based on the following: [

- *Subject attributes (users)*
  - *User ID*
  - *Password*
  - *Access type*
  - *Authorization*
  - *Location*
  - *Access time*
  - *Vault user account expiration date*
- *Object attributes (safes)*
  - *Name*
  - *File types*].

FDP_ACF.1(1).2

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

- *Access to view the safes can be limited to users based on*
  - *The IP*[37] *address (location) which they are accessing the vault from*
  - *The time of day that they are accessing the vault from*
  - *The expiration date of the account*
- *Users with the "Add safes" authorization can view and create safes from the vault*
- *Users with the "Manage Server File Categories" can view the file types allowed within a safe*

FDP_ACF.1(1).3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [

[37] IP – Internet Protocol

- *Users that supply the correct UserID and password combination and have the correct vault authorizations can view safes in the vault*
- *Users with the following access types can view safes in the vault*
  - *EPVUser*
  - *PVWA*
  - *PSM*
  - *PSMUser*
  - *PSMPServer*
  - *CPM*
  - *ENE*[38]
  - *AIMAccount*
  - *AppProvider*
  - *OPMProvider*
  - *OPMUser*
  - *PIMProvider*
  - *POCAdmin*].

FDP_ACF.1(1).4

The TSF shall explicitly deny access of subjects to objects based on the [

- *IP address (location) on which they are attempting to access the vault*
- *time of day on which they are attempting to access the vault*
- *the expiration date of the account when attempting to access the vault*].

FDP_ACF.1(2) Security attribute based access control (Safe)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3(2) Static attribute initialization (Safe)

FDP_ACF.1(2).1

The TSF shall enforce the [*Safe Access Control Policy*] to objects based on the following: [

- *Subject attributes (safe members)*
  - *User ID*
  - *Permissions*
- *Object attributes (accounts/passwords and files)*
  - *account name*
  - *value/data*
  - *access rules*].

FDP_ACF.1(2).2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*Users with the permissions listed in the "Permissions" column of Table 11 can act upon the accounts and their values as stated in the "Object Operations (Account Name)" and "Object Operations (Value/Data)" columns in* Table 11].

Table 11 Safe Access Control Permissions

Permission	Object Operations (Account name)	Object Operations (Value/Data)
Use Accounts	Read	None
Retrieve Accounts	Read	Read
List Accounts	Read	None
Add accounts	Read, write, remove	None
Update password value	Read	Read, write

[38] ENE – Event Notification Engine

Permission	Object Operations (Account name)	Object Operations (Value/Data)
Update password properties	Read	None
Initiate CPM password management operations	Read	Read, write
Specify next password value	Read	Read, write
Rename Accounts	Read, write	None
Delete Accounts	Read, remove	None
Unlock Accounts	Read, write	None
Manage Safe	Read, write, remove	None
Manage Safe Members	Read	None
Backup Safe	Read	None
Move accounts/folders	Read	None

FDP_ACF.1(2).3

The TSF shall explicitly authorized access of subjects to objects based on the following additional rules: [*users must supply the correct UserID and password in order to access the contents of the safe*].

FDP_ACF.1(2).4

The TSF shall explicitly deny access of subjects to objects based on the [*the UserID and explicit access rules for each account/password given to that UserID*].

6.2.5 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 identification
FIA_UAU.2.1

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

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies
FIA_UID.2.1

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

6.2.6 Class FMT: Security Management

FMT_MOF.1(1) Management of security function behaviors (Vault)
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security Roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1(1).1

The TSF shall restrict the ability to [determine the behavior of, disable, enable, modify the behavior of] the functions [*listed under the 'Security Functions Behavior Permissions' column of* Table 12] to [*the authorizations listed under the 'Authorizations' column of* Table 12].

Table 12 Management of Vault Security Function Behavior by Role

Authorizations	Security Function Behavior Permissions
Add Safes	Add safes to the vault
Audit Users	Track user activities in the vault
Add/Update Users	Add and update users, manage network areas, manage locations
Reset Users' Passwords	Reset a user's password
Activate Users	Activate or deactivate trusted network areas for users
Add Network Areas	Add, update, and remove network areas that specify where the vault can be accessed
Manage Directory Mapping	Add, update, and remove directory maps that manage users transparently
Manage Server File Categories	Add, update, and remove file categories
Backup All Safes	Run backup procedures
Restore All Safes	Run restore procedures

FMT_MOF.1(2) Management of security function behaviors (Safe)
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security Roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1(2).1

The TSF shall restrict the ability to [determine the behavior of, disable, enable, modify the behavior of] the functions [*listed under the 'Security Functions Behavior Permissions' column of* Table 13] to [*the permissions listed under the 'Permissions' column of* Table 13].

Table 13 Management of Safe Security Function Behavior by Role

Permissions	Security Function Behavior Permissions
Use Accounts	Access and use the accounts saved within a safe
Retrieve Accounts	Access and use the accounts saved within a safe; View the plaintext version of a password associated with the account; Save files to the safe; Open files located in the safe
List Accounts	View the accounts and files located on the safe; Cannot access the account or file

Permissions	Security Function Behavior Permissions
Add Accounts	Add accounts and associated passwords to the safe; Update account properties
Update Password Value	Change the password associated with an account; Undelete an account; Save files to the safe;
Update Password Properties	Update account properties (does not include password)
Initiate CPM Password Management Operations	Initiate password management operations through the CPM – includes changing, verifying, and reconciling passwords
Specify Next Password Value	Specify the next password to be used when the CPM changes the password value
Rename Accounts	Rename existing accounts in the safe
Delete Accounts	Remove existing accounts in the safe
Unlock Accounts	Unlock existing accounts and files in the safe
Manage Safe	Update, recover, and remove a safe from the vault
Manage Safe Members	Add, remove, and update members of the safe; Manage account permissions
Backup Safe	Create a backup of a safe and its contents
View Audit Log	View account and user activity in the safe; Does not have permissions to view or use accounts
View Safe Members	View members of the safe and their permissions
Authorize Password Request	Give confirmation to a user requesting access to the safe; View the accounts and files located on the safe;
Access Safe without Confirmation	Access a safe without being a member of the safe and no need to request permission
Create Folders	Create folders on the safe
Delete Folders	Delete folders on the safe
Move accounts/folders	Move accounts and folders in the safe

FMT_MSA.1(1) Management of security attributes (Vault)

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).1

The TSF shall enforce the [*Vault Access Control Policy*] to restrict the ability to [selection: query, modify, delete, *create*] the security attributes [*security attribute listed in the "Attributes" column of Table 14*] to [*the users with the authorizations listed in the "Authorizations" column of Table 14*].

Table 14 Management of Vault Security Attributes

Operation	Attributes	Authorizations
<u>Query</u>	*UserID*	Audit Users Add/Update Users
	Access type	
	Authorization	
	Location	
	Access time	
	Account expiration date	
<u>Modify</u>	*Password*	Audit Users Reset Users' Passwords Activate Users
	Account expiration date	
<u>Modify</u>	*Access type*	Add/Update Users
	Authorization	
	Access time	
	Account expiration date	
<u>Modify</u>	*Location*	Add Network Areas
<u>Modify</u>	*Safe file type*	Manager Server File Categories
<u>Delete</u>	*UserID*	Add/Update Users
<u>Create</u>	*Safe name*	Add Safes

FMT_MSA.1(2) Management of security attributes (Safe)

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(2).1

The TSF shall enforce the [*Safe Access Control Policy*] to restrict the ability to [selection: <u>query, modify, delete, *create*</u>] the security attributes [*security attribute listed in the "Attributes" column of Table 15*] to [*the users with the permissions listed in the "Permissions" column of Table 15*].

Table 15 Management of Safe Security Attributes

Operation	Attributes	Permissions
Query	*User ID*	Manage Safe Members View Safe Members
	User Permissions	
Query	*Account name*	Use Accounts Retrieve Accounts List Accounts Add Accounts Update Password Value Update Password Properties Initiate CPM Password Management Operations Rename Accounts Delete Accounts Unlock Accounts Move Accounts/Folders
Query	*Value/Data*	Retrieve Accounts Update Password Value Initiate CPM Password Management Operations
Query/Modify	*Permissions*	Manage Safe Members
	Access rules	
Modify	*Account name*	Rename Accounts
Modify	*Value/Data*	Update Password Value Initiate CPM Password Management Operations
Delete	*Account name*	Delete Accounts Manage Safe
	Value/Data	
Delete	*User ID*	Manage Safe Members
Create	*User ID*	Manage Safe Members
Create	*Account name*	Add Accounts
Create	*Value/Data*	Add Accounts Specify Next Password Value
Create	*Access rules*	Manage Safe Members

FMT_MSA.3(1) Static attribute initialization (Vault)

Hierarchical to: No other components.
Dependencies: FMT_MSA.1(1) Management of security attributes (Vault)
FMT_SMR.1 Security roles

FMT_MSA.3(1).1

The TSF shall enforce the [*Vault Access Control Policy*] to provide [restrictive] default values for security attributes that are used to enforce the SFP[39].

FMT_MSA.3(1).2

The TSF shall allow **users with** the [*Add Safe authorization*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3(2) Static attribute initialization (Safe)

Hierarchical to: No other components.
Dependencies: FMT_MSA.1(2) Management of security attributes (Safe)
FMT_SMR.1 Security roles

FMT_MSA.3(2).1

The TSF shall enforce the [*Safe Access Control Policy*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3(2).2

The TSF shall allow **users with** the [*Manage Safe permission*] 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: [*User management, authentication management, access control management, audit log management, vault management, configuration management, safe management, account management, file management*].

FMT_SMR.1 Security roles

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1

The TSF shall maintain the roles [*custom roles with administrator-defined permissions*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

[39] SFP – Security Functional Policy

6.2.7 Class FPT: Protection of the TSF

FPT_APW_EXT.1 Protection of Stored Credentials
Hierarchical to: No other components.
Dependencies: No other components.
FPT_APW_EXT.1.1
The TSF shall store credentials in non-plaintext form
FPT_APW_EXT.1.2
The TSF shall prevent the reading of plaintext credentials from unauthorized users.

FPT_FLS.1 Failure with preservation of secure state
Hierarchical to: No other components.
Dependencies: No other components.
FPT_FLS.1.1
The TSF shall preserve a secure state when the following types of failures occur: [

- *Destruction of the vault (physical or logical)*
- *Loss in network connectivity*].

FPT_ITT.1 Basic Internal TSF Data Transfer Protection
Hierarchical to: No other components.
Dependencies: No other components.
FPT_ITT.1.1
The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.

6.2.8 Class FRU: Resource Utilization

FRU_FLT.1 Degraded Fault Tolerance
Hierarchical to: No other components.
Dependencies: FPT_FLS.1 Failure with preservation of secure state

FPT_FLT.1.1

The TSF shall ensure the operation of [*access to the EPV, its safes, and the accounts and files within the safes*] when the following failures occur: [

- *Destruction of the vault (physical or logical)*
- *Loss in network connectivity*].

6.2.9 Class FTA: TOE Access

FTA_SSL.3 TSF-Initiated Termination
Hierarchical to: No other components.
Dependencies: No other components.
FTA_SSL.3.1

The TSF shall terminate an interactive session after:

- For the PrivateArk Client: [*a default period of 30 minutes of inactivity or an administrator-defined period of inactivity*];
- For the PVWA Interface: [*a non-configurable period of 10 minutes of inactivity*].

FTA_TAB.1 Default TOE Access Banners
Hierarchical to: No other components.
Dependencies: No other components.
FTA_TAB.1.1

Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

FTA_TSE.1 TOE Session Establishment
Hierarchical to: No other components.
Dependencies: No other components.
FTA_TSE.1.1

The TSF shall be able to deny session establishment based on [

- *Incorrect User ID*
- *Incorrect Password*
- *Attempting to access the TOE through an interface while having the incorrect access type*
- *Location (IP Address) of attempted session establishment*
- *Account expiration date*]

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements listed in Table 16 are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2.

Table 16 EAL2 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 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.
[If ASE_TSS.2 is found to apply to the evaluation, provide a description of how TOE protects itself against interference and logical tampering, and bypass.]

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements. Table 17 lists all SFRs claimed within this Security Target.

Table 17 Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SAR.3	Selectable Audit Review
	FAU_STG.1	Protected Audit Storage
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_ACC.1(1)	Subset access control (Vault)
	FDP_ACC.1(2)	Subset Access Control (Safe)
	FDP_ACF.1(1)	Security attribute based access control (Vault)
	FDP_ACF.1(2)	Security attribute based access control (Safe)
Identification and Authentication	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1(1)	Management of security function behavior (Vault)
	FMT_MOF.1(2)	Management of security function behavior (Safe)
	FMT_MSA.1(1)	Management of security attributes (Vault)
	FMT_MSA.1(2)	Management of security attributes

TOE Security Functionality	SFR ID	Description
		(Safe)
	FMT_MSA.3(1)	Static attribute initialization (Vault)
	FMT_MSA.3(2)	Static attribute initialization (Safe)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_APW_EXT.1	Protection of Stored Credential
	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITT.1	Basic Internal TSF Data Transfer Protection
Resource Utilization	FRU_FLT.1	Degraded Fault Tolerance
TOE Access	FTA_SSL.3	TSF-Initiated Termination
	FTA_TAB.1	Default TOE Access Banner
	FTA_TSE.1	TOE Sessions Establishment

7.1.1 Security Audit

The Security Audit function provides the TOE with the functionality of generating audit records. Typical audit records that can be accessed by a user with the correct authorizations include Privileged Account Inventory, Safe Lists, User Lists, and User Activities. As TOE users access, manage, and configure the TOE, their activities are tracked. When an Auditor user (TOE user with the "View audit" authorization) generates an "Activity Log", the Auditor will see the various activities performed by TOE users in an organized list. The audit list contains the columns and information listed in Table 18.

Table 18 Audit Record Contents

Field	Content
Time	The time the activity was performed (The date and time are displayed in the time zone of the EPV)
User	The full name of the user who performed the activity
Action	The activity performed by the user
Safe	The safe where the privileged account is stored
Target	The privileged account that was used in the activity
Target Platform	The unique ID of the platform that was allocated to the privileged account used in the activity.
Target System	The remote system where the privileged account was used.

Field	Content
Target Account	The name of the target account where the privileged account was used.
New Target	The new location/name of an account on which the activity was performed and extra details about the activity that was performed.
Reason	The reason given by the user for performing the activity
Alert	An indication that this activity prompted an alert
Request ID	The unique ID of the request that was created in order to retrieve the privileged account used in the activity
Client ID	The unique ID of the client used in the activity

Furthermore, once an Activity Log has been generated, the results can be filtered with general filters, filters by target system, activities, and history of the activity. Each item listed in Table 18 above can be individually filtered. A filter can be placed on each individual action taken by the TOE user. Those actions include:

- privileged account access,
- approval workflow,
- privileged account management,
- privileged account auto-detection,
- safe management,
- member management,
- user login,
- user/group/location management,
- vault system administration,
- reports management,
- file access, and
- file management

When an audit record is requested, it will be generated by the TOE and stored on the local host server within a reports safe dedicated for audit records. Only users with the correct authorizations and permission are capable of accessing the contents of the safe. The records safe and its contents are secured by the EPV by individual encryption keys. Each individual file is encrypted with its own, unique encryption key. Then the records safe is encrypted with its own, unique encryption key. This will prevent any unauthorized access, deletion, or modification to the records.

The start-up and shut down events of the TOE are provided with the support of the TOE environment. Each TOE component is registered as an OS service. Upon start-up and shutdown, events are stored in the OS event logs. These logs are viewed by authorized administrators using the appropriate tools.

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

7.1.2 Cryptographic Support

The TOE implements FIPS 140-2 Approved cryptographic algorithms to support cryptographic functionality such as encryption, decryption, and hashing. The cryptographic module within the TOE generates a unique AES 256-bit key for each individual safe located in the EPV. Additionally each account and file located within each safe is protected by a unique AES 256-bit key. AES, RSA, and HMAC are all used by the TOE when performing a TLS or SSH session with a remote machine. All AES, RSA, and HMAC keys are generated either with an SP 800-90 DRBG, or with the ANSI X9.31 RNG[40].

Each of the cryptographic algorithms supported by the TOE have been tested and certified by the CAVP[41]. Each algorithm has been awarded a certificate number. Table 10 above lists each algorithm in use by the TOE and their associated algorithm certificate.

The TOE is responsible for destroying all ephemeral keying material generated within the TOE boundary. The TOE uses FIPS 140-2 Approved zeroization methods in order to destroy all keys and other critical parameters generated by the TOE at the appropriate time.

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.4, FCS_COP.1

7.1.3 User Data Protection

The TOE provides the User Data Protection security function to manage user access and interaction with safes and accounts stored on the EPV. The TOE enforces two access control policies which limit access to the safes located on the EPV (Vault Access Control Policy) and further limit access to the accounts and files stored within the safes (Safe Access Control Policy). Access to the vault and safes are enforced by user account authorizations and permissions. An operator attempting to access the EPV or Safes with the incorrect authorizations and permissions will be denied access.

Operators can access the safe through one of the many TOE component interfaces including: PrivateArk Client and Web Client, PVWA, PSM, PSMP, CPM, AIM, and OPM. Access to the EPV through these interfaces requires the correct access type associated with each TOE user. Once granted access to the EPV, the users with the correct authorizations can manage the vault and the safes within the vault. This includes the creation of safes and the management of file types allowed within each safe. TOE users can be denied access to the vault if they are attempting to access the vault from an interface in which they do not have the correct access type for. Additionally, vault access can be limited to TOE user based on the time of day, location of access, or account expiration date.

In order for a user to access the contents within a safe, they must be added as a safe member by a safe member with the “Manage Safe Members” permission. Each safe member is given safe permissions which allow them to read, write, and remove accounts and files located within the safe. Some safe members will be allowed to view detailed account information while others may only be able to run an audit report on the safe. Users can be denied access to specific accounts and files located within a safe based on the access rules given to an account or file.

TOE Security Functional Requirements Satisfied: FDP_ACC.1(1), FPD_ACC.1(2), FDP_ACF.1(1), FDP_ACF.1(2)

7.1.4 Identification and Authentication

TOE users must provide the correct username and password associated with an external LDAP account. The TOE must successfully identify and authenticate a user prior to allowing any actions on their behalf. The TOE identifies and authenticates the user by passing the username and password combination to the LDAP server for validation.

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

[40] RNG – Random Number Generator

[41] CAVP – Cryptographic Algorithm Validation Program.

7.1.5 Security Management

Management of the TOE can be defined as "granular". Each TOE user that is granted access to the TOE is provided with a profile, which defines the user's access rights, management rights, and action rights within the TOE. Within the EPV, a list of authorizations provided to each user defines the actions that they can take within the vault. Further, within each safe, a safe member is granted a list of permissions which controls how they can interact with the accounts and files within the safe. When first creating a user in the vault and when providing them access to a safe, the TOE enforces restrictive default values by not providing the user with any authorizations or permissions. Authorizations are added by the TOE user creating the new user within the EPV and permissions are given to the new user when adding them as a safe member to one or many safes.

Due to the granular control of TOE user authorizations and permissions, the TOE does not inherently define security roles.

The TOE defines restrictive default values for the Vault Access Control Policy and Safe Access Control Policy. Only users explicitly granted permissions have access to safes and account/password files.

TOE Security Functional Requirements Satisfied: FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.3(1), FMT_MSA.3(2), FMT_SMF.1, FMT_SMR.1.

7.1.6 Protection of the TSF

The TOE employs a multi-layered encryption scheme in order to protect the credentials stored within the EPV. The three layers of encryption employed by the EPV are the vault layer, safe layer, and account/file layer. All accounts, files, safes, and even the vault itself are encrypted with unique encryption keys. Each account and file stored within a safe is encrypted with its own file encryption key. Each safe is encrypted with its own safe key. Then the vault itself is encrypted with a vault key. Each key is stored within the vault in its own safe, providing further protection of the encryption keys. Access to the plaintext version of the credentials stored within a vault is limited to the authorized users of the safe with the "Retrieve Accounts" safe privilege.

The TOE provides a trusted internal channel for all components of the TOE. The TOE utilizes a patented communications protocol developed by CyberArk, which employs AES-256 for confidentiality and HMAC SHA-1 for integrity. The TOE components all communicate with one another through a variety of ports which ensures that all of their communication is secure and logically separate.

The TOE provides seamless switching between the main EPV and a back-up (Disaster Recovery) Vault if a failure to the main EPV occurs. Types of failures include physical and logical destruction of the EPV (or its host server) or loss of network connectivity. This transparent failover preserves a secure state of the TOE.

TOE Security Functional Requirements Satisfied: FPT_APW_EXT.1, FPT_FLS.1, FPT_ITT.1

7.1.7 Resource Utilization

The TOE provides seamless switching between the main EPV and a back-up (Disaster Recovery) Vault if a failure to the main EPV occurs. Types of failures include physical and logical destruction of the EPV (or its host server) or loss of network connectivity. This transparent failover ensures that regular access to the TOE and its functions is maintained.

TOE Security Functional Requirements Satisfied: FRU_FLT.1.

7.1.8 TOE Access

TOE users attempting to access the TOE through the PVWA or PrivateArk client will encounter a display banner prior to being able to log into the TOE. The banner provides access to an advisory warning message regarding the unauthorized use of the TOE. Access to the TOE will be limited to users that provide the correct username and password combination.

Restrictions can be placed on a TOE user, which will deny them access to the TOE. The location from which a TOE user is attempting to access the TOE can be used to limit access to the TOE. Administrators can also place an account expiration date onto a user account. Once the account has expired, the user will not be allowed to access the TOE. Lastly, if the user does not have the correct access type to access the TOE from a given interface, they will be denied access to the TOE.

Users must actively interact with the TOE in order to avoid session termination. If the user account has not interacted with the TOE for 10 minutes via the PVWA, or for an administrator-defined inactivity period (default of 30 minutes) via the PrivateArk Client, the session will terminate and the user will be logged out of the TOE. The user must proceed with the login process in order to regain access to the TOE.

TOE Security Functional Requirements Satisfied: FTA_SSL.3. FTA_TAB.1, FTA_TSE.1

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 extended and Part 3 conformant of the Common Criteria Standard for Information Technology Security Evaluations, Version 3.1 Revision 3. This ST does not conform to a PP.

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 and 8.2.2 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 19 maps all threats to all objectives.

Table 19 Threats: Objectives Mapping

Threats	Objectives	Rationale
T.ADMIN_ERROR An administrator may incorrectly configure the TOE resulting in ineffective security mechanisms.	OE.TRUSTED_ADMIN Trusted TOE Administrators must follow and apply all administrator and configuration guidance.	OE.TRUSTED_ADMIN counters this threat by ensuring that administrators follow all administrative guidance.
T.AUDIT_COMPROMISE A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future records from being recorded, thus masking a user's actions.	O.AUDIT The TOE will provide the capability to detect security relevant events and record them to the audit trail.	O.AUDIT counters this threat by ensuring that unauthorized attempts to access the TOE are recorded.
	O.AUDIT_STORAGE The TOE will provide a secure method of storing local audit records.	O.AUDIT_STORAGE counters this threat by ensuring that only authorized users are allowed to access stored audit records, and that audit records are encrypted within local storage.
T.DATA_COMPROMISE An unauthorized user may read, modify, delay, or destroy security critical TOE data stored on the TOE or being transmitted between physically separated parts of the TOE.	O.CRYPTO The TOE will provide FIPS 140-2 Approved cryptographic algorithms and procedures to TOE users during operation of the TOE.	O.CRYPTO counters this threat by providing encryption services available to authorized users and/or user applications.
	O.PROTECT_COMM The TOE will provide protected communication channels for parts of the distributed TOE.	O.PROTECT_COMM counters this threat by providing protected communication channels for parts of the distributed TOE.
	O.TOE_ADMIN The TOE will provide mechanisms to ensure that only authorized	O.TOE_ADMIN counters this threat by ensuring that only trusted administrators are able to

Threats	Objectives	Rationale
	administrators are able to configure the TOE security functions attributes.	change the security functions and attributes stored on the TOE.
	O.VAULT The TOE will provide mechanisms to ensure that stored credentials are not stored in plaintext and are protected from unauthorized access	O.VAULT counters this threat by encrypting all stored credentials.
T.MASQUERADE A malicious user, process, or external IT entity may masquerade as an authorized entity to gain unauthorized access to data or TOE resources.	O.USER_AUTHEN The TOE will uniquely identify and authenticate users prior to allowing access to TOE functions and data.	O.USER_AUTHEN counters this threat by ensuring that the TOE is able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
	O.BANNER The TOE will present an access banner to TOE users prior to accessing the TOE that defines acceptable use of the TOE	O.BANNER counters this threat by providing a warning message to users about unauthorized use of the TOE prior to logging in.
T.UNAUTHORIZED _ACCESS A user may gain unauthorized access (view, modify, delete) to user data.	O.ACCESS The TOE will ensure that only authorized users may gain access to it and the resources that it controls.	O.ACCESS counters this threat by ensuring that users gain only authorized access to it and to resources that it controls.
	O.ROBUST_ACCESS The TOE will implement mechanisms that can deny or suspend session establishment	O.ROBUST_ACCESS counters this threat by ensuring only authorized users are allowed to connect to the TOE. O.ROBUST_ACCESS counters this threat by automatically closing inactive sessions.
	O.PERMISSIONS The TOE will provide a method to separate and restrict the abilities of individual TOE users	O.PERMISSIONS counters this threat by assigning users different permissions which relate to the data which they are allowed to access.
T.UNIDENTIFIED _ACTIONS The administrator may fail to notice potential security violations, thus preventing the administrator from taking action against a possible security violation.	O.AUDIT_REVIEW The TOE will provide the capability for only authorized users to view audit information.	O.AUDIT_REVIEW counters this threat by providing the capability for only authorized administrators to view audit information.
T.DISASTER Operation or access to the TOE may suddenly fail, rendering the TOE useless	O.FAIL_SECURE The TOE will provide a method to continue secure operations during a catastrophic TOE failure	O.FAIL_SECURE counters this threat by providing a seamless transition to a working version of the TOE.

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 Assumptions

Table 20 maps all assumptions to environmental objectives.

Table 20 Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.	NOE.PHYSICAL The TOE environment must provide physical security commensurate with the value of the TOE and the data it contains.	NOE.PHYSICAL satisfies the assumption by ensuring that the TOE environment provides physical security commensurate with the value of the TOE and the data it contains.
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 by performing integrity checks to ensure external interference or tampering has not occurred.
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 by providing reliable timestamps provided by the TOE environment hardware clock.
A.TRUSTED_ADMIN TOE Administrators are non-hostile and are trusted to follow and apply all administrator guidance.	OE.TRUSTED_ADMIN Trusted TOE Administrators must follow and apply all administrator and configuration guidance.	OE.TRUSTED_ADMIN satisfies the assumption by ensuring that only trusted administrators follow and apply all administrator guidance.
A.HARDEN The EPV component of the TOE will be installed on a hardened instance of Windows	OE.HARDENED The TOE environment must provide a hardened version of Windows for the installation of EPV.	OE.HARDENED satisfies the assumption by ensuring a hardened version of Windows is provided for the installation of the EPV.
A.ACCESS Access to the TOE will be provided by a reliable network connection	OE.NETWORK The TOE environment must provide a consistent network connection to the TOE.	OE.NETWORK satisfies the assumption by ensuring a consistent network connection to the TOE will always be provided.
A.INSTALL TOE components will be installed onto a compatible Operating System	OE.OS The TOE environment must provide a compatible Windows or Linux Operating System version for the installation of TOE components.	OE.OS satisfies the assumption by ensuring that a compatible Window or Linux Operating System will be provided for the installation of TOE components.
A.INTERNAL_SERVICES All LDAP and remote systems that the TOE communicates with should be located on the same	OE.INTERNAL_SERVICES LDAP servers and remote systems accessed by the TOE are located on the same internal	OE.INTERNAL_SERVICES satisfies this assumption by ensuring that LDAP and remote systems accessed by the TOE are

Assumptions	Objectives	Rationale
internal network as the TOE. Users on this network are assumed to be non-hostile.	network as the TOE. Users on this network are non-hostile.	located within the same internal network as the TOE. Users on this network are non-hostile.

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

Two extended SFRs were created to support the advanced functionality of the PAS Solution.

FPT_APW was created to specifically address the non-plaintext storage of user credentials on the TOE. The CC Part 2 FPT SFRs do not cover the non-plaintext storage of user credentials. In this case, all user credentials are being stored on the TOE in encrypted form. As a result, the FPT SFRs do not apply. The purpose of this extended requirement is to describe the secure, encrypted storage of user credentials on the TOE.

This requirement exhibits functionality that can be easily documented in the ADV assurance evidence and thus does not require any additional Assurance Documentation.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no Extended SARs defined for 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 21 maps all objects to SFRs.

Table 21 Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE will ensure that only authorized users may gain access to it and the resources that it controls.	FDP_ACC.1(1) Subset access control (Vault)	The requirement meets the objective by enforcing the Vault Access Control Policy on all subjects and all named objects and all operations among them. The policy specifies the access rules between all subjects and all named objects controlled by the TOE. While authorized users are

Objective	Requirements Addressing the Objective	Rationale
		trusted to some extent, this requirement ensures only authorized access is allowed to named objects.
	FDP_ACC.1(2) Subset Access Control (Safe)	The requirement meets the objective by enforcing the Safe Access Control Policy on all subjects and all named objects and all operations among them. The policy specifies the access rules between all subjects and all named objects controlled by the TOE. While authorized users are trusted to some extent, this requirement ensures only authorized access is allowed to named objects.
	FDP_ACF.1(1) Security attribute based access control (Vault)	The requirement meets the objective by specifying the Vault Access Control 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.
	FDP_ACF.1(2) Security attribute based access control (Safe)	The requirement meets the objective by specifying the Safe Access Control 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.
O.AUDIT The TOE will provide the capability to detect security relevant events and record them to the audit trail.	FAU_GEN.1 Audit data generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined events, including relevant details about the event.
	FAU_GEN.2 User Identity Association	The requirement meets the objective by ensuring that the TOE associates each auditable event with the identity of the user that caused the event.
O.AUDIT_REVIEW	FAU_SAR.2	The requirement meets the

Objective	Requirements Addressing the Objective	Rationale
The TOE will provide the capability for only authorized users to view audit information.	Restricted audit review	objective by ensuring that only authorized users are able to review logs.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides the ability to review logs.
	FAU_SAR.3 Selectable Audit Review	The requirement meets the objective by ensuring the TOE provides an organized method to review audit records
O.AUDIT_STORAGE The TOE will provide a secure method of storing local audit records.	FAU_STG.1 Protected Audit Storage	The requirement meets the objective by ensuring that only authorized users are allowed to access stored audit records, and by encrypting stored audit records.
O.CRYPTO The TOE will provide FIPS 140-2 Approved cryptographic algorithms and procedures to TOE users during operation of the TOE.	FCS_CKM.1 Cryptographic key generation	The requirement meets the objective by ensuring that the TOE can generate FIPS-Approved cryptographic keys for use during cryptographic operations.
	FCS_CKM.4 Cryptographic key destruction	The requirement meets the objective by ensuring that the TOE destroys cryptographic keys when no longer in use using FIPS-Approved methods
	FCS_COP.1 Cryptographic operation	The requirement meets the objective by ensuring that the TOE provides FIPS-Approved confidentiality and integrity services for the TOE.
O.USER_AUTHEN The TOE will uniquely identify and authenticate users prior to allowing access to TOE functions and data.	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that every user is authenticated before the TOE performs any TSF-mediated actions on behalf of that user.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that every user is identified before the TOE performs any TSF-mediated actions on behalf of that user.
O.PROTECT_COMM The TOE will provide protected communication channels for parts of the distributed TOE.	FPT_ITT.1 Basic Internal TSF Data Transfer Protection	The requirement meets the objective by protecting data being transferred between TOE components from disclosure and

Objective	Requirements Addressing the Objective	Rationale
		modification
O.BANNER The TOE will present an access banner to TOE users prior to accessing the TOE that defines acceptable use of the TOE	FTA_TAB.1 Default TOE Access Banner	The requirement meets this objective by presenting an access banner to all TOE users prior to being able to login to the TOE
O.TOE_ADMIN The TOE will provide mechanisms to ensure that only authorized administrators are able to configure the TOE security functions attributes.	FMT_MSA.1(1) Management of security attributes (Vault)	The requirement meets the objective by ensuring that only administrators with the ability to manage security attributes for the vault may do so..
	FMT_MSA.1(2) Management of security attributes (Safe)	The requirement meets the objective by ensuring that only administrators with the ability to manage security attributes for the safe may do so.
	FMT_MSA.3(1) Static attribute initialisation (Vault)	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_MSA.3(2) Static attribute initialisation (Safe)	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 users with roles to provide access to TSF management functions and data.
O.ROBUST_ACCESS The TOE will implement mechanisms that can deny or suspend session establishment	FTA_SSL.3 TSF-Initiated Termination	The requirement meets the objective by suspending currently active sessions that have been inactive for a configurable amount of time

Objective	Requirements Addressing the Objective	Rationale
	FTA_TSE.1 TOE Sessions Establishment	The requirement meets the objective by denying users access to the TOE based on user attributes
O.FAIL_SECURE The TOE will provide a method to continue secure operations during a catastrophic TOE failure	FPT_FLS.1 Failure with preservation of secure state	The requirement meets the objective by providing seamless failover over when a failure of the TOE occurs by preserving a secure state.
	FRU_FLT.1 Degraded Fault Tolerance	The requirement meets the objective by providing seamless failover over when a failure of the TOE occurs by preserving an operational state.
O.VAULT The TOE will provide mechanisms to ensure that stored credentials are not stored in plaintext and are protected from unauthorized access	FPT_APW_EXT.1 Protection of Stored Credential	The requirement meets the objective by ensuring all credentials stored on the TOE are encrypted. The requirement restricts unauthorized uses from viewing the plaintext credentials.
O.PERMISSIONS The TOE will provide a method to separate and restrict the abilities of individual TOE users	FMT_MOF.1(1) Management of security function behavior (Vault)	The requirement meets the objective by providing granular authorizations, which can be assigned to each user of the vault. A user can have none or all of the authorizations.
	FMT_MOF.1(2) Management of security function behavior (Safe)	The requirement meets the objective by providing granular permissions, which can be assigned to each member of a safe. A member can have none or all of the permissions.
	FMT_SMR.1 Security roles	The requirement meets the objective by associating the accumulated permissions of a TOE user to a defined role which provides access to different TSF management functions and data

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. While the System may monitor a hostile environment, it 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 System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment. The augmentation of ALC_FLR.1 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 22 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As Table 22 indicates, all dependencies have been met, or rationale has been provided as to why a particular dependency cannot be met.

Table 22 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1		FPT_STM.1 is not included because time stamps are provided by the environment. An environmental objective states that the TOE will receive reliable timestamps.
FAU_GEN.2	FAU_GEN.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.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.2	FAU_SAR.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FCS_CKM.1	FCS_CKM.4	✓	
	FCS_COP.1	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FDP_ACC.1(1)	FDP_ACF.1(1)	✓	
FDP_ACC.1(2)	FDP_ACF.1(2)	✓	
FDP_ACF.1(1)	FDP_ACC.1(1)	✓	
	FMT_MSA.3(1)	✓	
FDP_ACF.1(2)	FDP_ACC.1(2)	✓	
	FMT_MSA.3(2)	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FIA_UID.2	No dependencies	✓	
FMT_MOF.1(1)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MOF.1(2)	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(1)	FDP_ACC.1(1)	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(2)	FDP_ACC.1(2)	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(1)	FMT_MSA.1(1)	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(2)	FMT_MSA.1(2)	✓	
	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_APW_EXT.1	No dependencies	✓	
FPT_FLS.1	No dependencies	✓	
FPT_ITT.1	No dependencies	✓	
FRU_FLT.1	FPT_FLS.1	✓	
FTA_SSL.3	No dependencies	✓	
FTA_TAB.1	No dependencies	✓	
FTA_TSE.1	No dependencies	✓	

9 Acronyms

9.1 Acronyms

Table 23 lists the acronyms used throughout this document.

Table 23 Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
AIM	Application Identity Manager
ANSI	American National Standards Institute
API	Application Programming Interface
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
CPM	Central Policy Manager
DR	Disaster Recovery
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
ENE	Event Notification Engine
EPV	Enterprise Password Vault
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GB	Gigabyte
GUI	Graphical User Interface
HMAC	(keyed-) Hash Message Authentication Code
HTTPS	Secure Hyper-Text Transfer Protocol
IIS	Internet Information Services
IP	Internet Protocol
IT	Information Technology
JRE	Java Runtime Environment
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MS	Microsoft Services
NIST	National Institute of Standards and Technology

Acronym	Definition
OPM	On-demand Privileges Manager
OS	Operating System
OSP	Organizational Security Policy
PACLI	PrivateArk Vault CLI
PAS	Privileged Account Security
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PP	Protection Profile
PSM	Privileged Security Manager
PSMP	Privileged Security Manager SSH Proxy
PVWA	Password Vault Web Access
RADIUS	Remote Authentication Dial In User Server
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RDS	Remote Desktop Service
RHEL	Red Hat Enterprise Linux
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SAS	Serially Attached SCSI
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SDK	Software Development Kit
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transmission Layer Security

Acronym	Definition
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Security Specification
UDP	User Datagram Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network
WS	Web Services

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