# National Information Assurance Partnership


TM

# Common Criteria Evaluation and Validation Scheme Validation Report

# CyberArk Privileged Access Security – Digital Vault Server Including Enterprise Password Vault (EPV) v10.4

## Report Number: CCEVS-VR-11004-2019

**Dated: September 30, 2019**

**Version: 1.0**

**National Institute of Standards and Technology**
**Information Technology Laboratory**
**100 Bureau Drive**
**Gaithersburg, MD 20899**

**Department of Defense**
**National Security Agency**
**9800 Savage Road**
**Fort Meade, MD 20755-6940**

## ACKNOWLEDGEMENTS

**Validation Team**

Daniel Faigin

Marybeth Panock

**Evaluation Team**

Eve Pierre

Cheryl Dugan

**Common Criteria Testing Laboratory**

DXC
10830 Guilford Road, Suite 307
Annapolis Junction, Maryland 20701

# 1. EXECUTIVE SUMMARY

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the CyberArk Privileged Access Security – Digital Vault Server Including Enterprise Password Vault (EPV) v10.4, the Target of Evaluation (TOE), performed by DXC. It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by DXC of Annapolis Junction, MD in accordance with the United States evaluation scheme and completed on September 25, 2019. The information in this report is largely derived from the ST, the Evaluation Technical Report (ETR) and the functional testing report. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated September 2012 at Evaluation Assurance Level 1, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, Revision 4, September 2012 – and the NIAP Protection Profile for Application Software v1.2; April 22, 2016.

CyberArk Privileged Access Security – Digital Vault Server Including Enterprise Password Vault (EPV) v10.4, the TOE, is a software-based solution that runs on Windows and is the core component of CyberArk's Privileged Access Security (PAS) Solution. PAS enables organizations to secure, provision, control, and monitor all activities associated with privileged identities used in enterprise systems and applications. EPV securely manages, stores and controls access to privileged accounts.

The Evaluation Team performed an analysis of the international interpretations of the CC, CEM and determined that none of the international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all International interpretations with effective dates on or before June 1, 2019.

# 2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

## Table 1: Evaluation Identifiers

| Item | Identifier |
|---|---|
| Evaluation Scheme | United States NIAP Common Criteria Evaluation and Validation Scheme |
| Target of Evaluation | CyberArk Privileged Access Security – Digital Vault Server Including Enterprise Password Vault (EPV) v10.4 |
| Protection Profile | Protection Profile for Application Software v1.2; April 22, 2016 |
| Security Target | CyberArk Software Ltd. Privileged Access Security – Digital Vault Server including Enterprise Password Vault (EPV) v10.4 Security Target, version 0.17 |
| Date of evaluation | September 30, 2019 |
| Evaluation Technical Report | CyberArk Privileged Account Security - Digital Vault Server Including Enterprise Password Vault (EPV) v10.4 Evaluation Technical Report, v0.2 |
| Assurance Activity Report | Assurance Activity Report for CyberArk Privileged Account Security - Digital Vault Server Including Enterprise Password Vault (EPV) v10.4, v1.0 |
| Conformance Result | 1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, September 2012 Version 3.1 Revision 4<br>2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, September 2012 Version 3.1 Revision 4<br>3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, September 2012 Version 3.1 Revision 4.<br>4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, September 2012 Version 3.1 Revision 4.<br>The following CC conformance:<br>• Part 2 extended<br>• Part 3 extended<br>• Protection Profile for Application Software v1.2; April 22, 2016 conformant. |
| Common Criteria version | Common Criteria for Information Technology Security Evaluation Version 3.1, Revision 4, September 2012 |
| Common Evaluation Methodology (CEM) version | CEM version 3.1 R4, September 2012 |
| Sponsor | CyberArk Software Ltd. |
| Developer | CyberArk Software Ltd. |
| Evaluators | Eve Pierre, Cheryl Dugan |

| Item | Identifier |
|---|---|
| Validation Team | Daniel Faigin, Marybeth Panock |

# 3. SECURITY POLICY

The TOE is a software only product that manages the secure storage and access to privileged account files, and to the administrator and session activity files. The privileged account files are used by applications to connect to target machines.

Enterprise Password Vault (EPV) manages the secure storage and access to privileged account files, and to the administrator and session activity files.

Any data leakage across the TOE may cause severe damage to the organization and therefore must be prevented.

# 4. SECURITY PROBLEM DEFINITION

### Assumptions

The ST identified the following security assumptions:

**TABLE 1: TOE ASSUMPTIONS**

| Assumption Name | Assumption Definition |
|---|---|
| A.PLATFORM | The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE |
| A.PROPER_USER | The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy. |
| A.PROPER_ADMIN | The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy. |

### Threats

The ST identified the following threats addressed by the TOE:

**TABLE 2: TOE THREATS**

| Threat Name | Threat Definition |
|---|---|
| T.NETWORK_ATTACK | An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it. |
| T.NETWORK_EAVESDROP | An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints. |
| T.LOCAL_ATTACK | An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local |

| | |
|---|---|
| | communications. |
| T.PHYSICAL_ACCESS | An attacker may try to access sensitive data at rest. |

## Organizational Security Policies

The Security Target identifies the following Organizational Security Policies (OSPs) to which the TOE must comply.

**TABLE 3: ORGANIZATIONAL SECURITY POLICIES**

There are no Organizational Security Policies for the application.

# 5. ARCHITECTURAL INFORMATION

## Physical Scope and Boundary

The TOE Boundary includes the CyberArk developed EPV software, a separately installed Version Check tool, and the third-party software included in the TOE installation package. Any third-party source code or software that EPV has modified is considered TOE software.

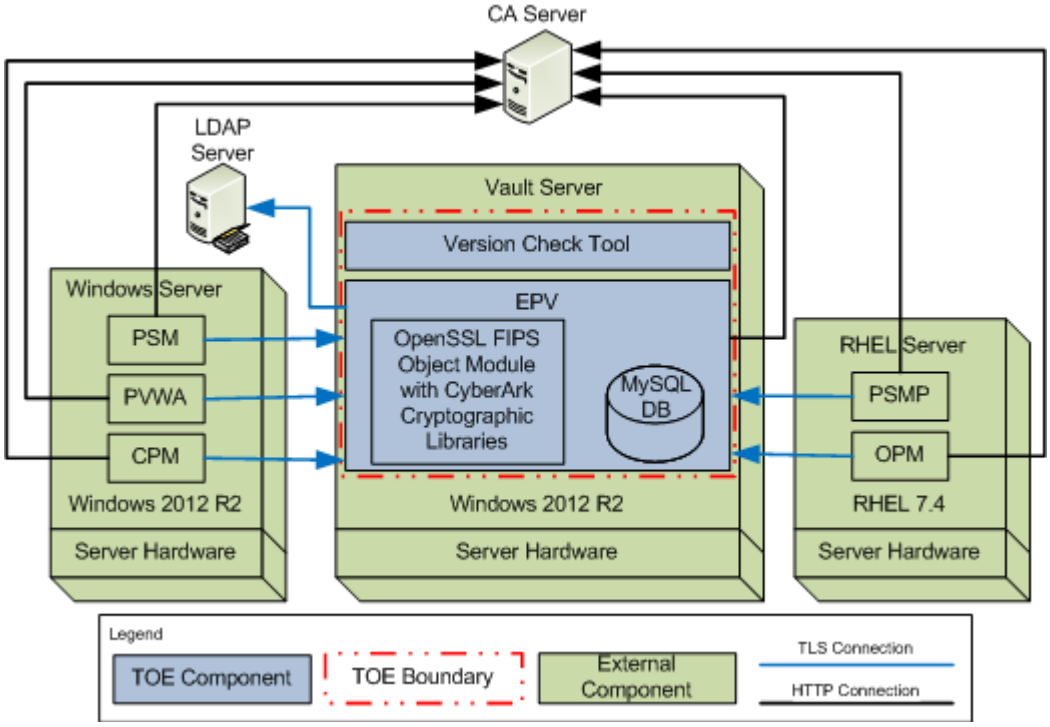


FIGURE 1 TOE BOUNDARY

The TOE is software-only and is comprised of the EPV application, which is compiled with OpenSSL FIPS Object Module v2.0.14 and a MySQL v5.6.15 DB. The TOE software, CyberArk EPV v10.4.1.27, must be installed on the Vault server. The installed software is comprised of the applications below.

- EPV is the application software that manages and controls access to the Vault, safes, and sensitive data. The EPV software is compiled with the following libraries:
  - The OpenSSL FIPS Object Module v2.0.14 with the two CyberArk cryptographic libraries, CyberArk PAS Cryptographic Library for Windows v1.0 and CyberArk Privileged Account Security TLS Library for Windows v1.0, provide cryptographic functionality for the TOE. EPV calls the OpenSSL FIPS Object Module v2.0.14 for the cryptographic services that will use the CyberArk libraries when required to secure sensitive data at rest and in transit, and to establish secure communications with other components in the OE.
  - The MySQL v 5.6.15 DB is used for the storage of sensitive data.

- CyberArk Version Check tool v1.5

## Components and Applications Required in the TOE Operational Environment

The TOE operates with the following components in its operational environment:

- Windows Server 2012 R2 Service Pack 1 (host platform) and .NET Framework 4.5.2
- LDAP Server
- CA Server
- Windows Server 2012 R2 with the following CyberArk PAS applications
  - Privileged Session Manager (PSM)
  - Password Vault Web Access (PVWA)
  - Central Policy Manager (CPM)
- RHEL Server 7.0 with the following CyberArk PAS applications
  - Privileged Session Manager SSH Proxy (PSMP)
  - On-Demand Privileges Manager (OPM)

## Logical Scope and Boundary

The logical scope of the TOE comprises the following security functions:

- **Cryptographic Support** — The TOE includes the OpenSSL FIPS Object Module v2.0.14 cryptographic module, which it uses to provide cryptographic services that include: encryption and decryption, hashing, digital signature generation and verification, cryptographic key generation, and random number generation.
- **User Data Protection** — The TOE ensures that only trusted OE components on the same isolated network can access its functions and/or data.
- **Identification and Authentication** — The TOE uses and X.509v3 certificates for TLS communications. The certificates are validated by the TOE and used for mutual authentication between the TOE and the Windows server PAS components, and the RHEL server PAS components. The TOE uses a certificate revocation list (CRL) to check the certificate revocation status and will not establish connections to the OE components when the CRL is not available
- **Security Management** — The TOE provides and restricts the capability to manage the TOE configuration, security functions, and other features of the TOE and OE components. The administrator can access the TOE management functions from the PVWA component running on Windows Server in the Operational Environment.
- **Privacy** — The TOE does not store or transmit any Personally Identifiable Information (PII).
- **Protection of the TSF** — The TOE provides protection of the TSF as follows:

- Does not map memory to explicit addresses except for OpenSSL functions
- Does not allocate memory regions with write and execute permissions
- Does not write user-modifiable files to directories that contain executable files
- Is compiled with stack-based overflow protection enabled
- Uses standard platform APIs
- Uses only the third-party libraries required for its functionality
- Exceeds the anti-exploitation security features provided by the Windows OS.
- Does not map memory to explicit addresses except for OpenSSL functions
- Does not allocate memory regions with write and execute permissions
- Does not write user-modifiable files to directories that contain executable files
- Is compiled with stack-based overflow protection enabled
- Uses standard platform APIs
- Uses only the third-party libraries required for its functionality
- Exceeds the anti-exploitation security features provided by the Windows OS.
- The TOE runs a suite of self-tests at power-on and during operation.

- **Trusted Path/Channel —** The TOE uses TLS v1.2 over LDAP (LDAPS) to secure communication between itself and the LDAP server in the operational environment. It uses TLS to communicate with the required PAS components running on the Windows and RHEL server in the operational environment. The TOE also requires mutual authentication between itself and all OE components that are not on its host platforms.

# 6. DOCUMENTATION

The TOE includes the following guidance documents:

- CyberArk Software Ltd. Privileged Access Security – Digital Vault Server Including Enterprise Password Vault (EPV) v10.4 Security Target Version 0.17, September 25, 2019
- CyberArk: Privileged Access Security Installation Guide; Version 10.4
- CyberArk: Privileged Access Security System Requirements; Version 10.4
- CyberArk; Privileged Access Security End-user Guide; Version 10.4
- CyberArk; Privileged Access Security Reference Guide; Version 10.4
- CyberArk; Privileged Access Security Implementation Guide; Version 10.4
- CyberArk Software Ltd.; Privileged Access Security Enterprise Password Vault Architecture v10.4; Guidance Documentation Supplement; Version: 0.8

All documentation delivered with the product is relevant to and within the scope of the TOE.

# 7. IT PRODUCT TESTING

This section describes the testing efforts of the evaluation team.

### Evaluation team independent testing

The evaluation team conducted independent testing at the CyberArk facilities in Petach-Tikva, Israel. The evaluation team configured the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Protection Profile test procedures as a basis for creating each of the Independent tests as required by the Assurance Activities.

Each Assurance Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

### Vulnerability analysis

The evaluation team performed a vulnerability analysis of the TOE evidence and a search of publicly available information to identify potential vulnerabilities in the TOE. There were no identifiable vulnerabilities found at the time of certification. The analysis was performed on August 28, 2019.

# 8. RESULTS OF THE EVALUATION

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1R4. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R4.

DXC has determined that the product meets the security criteria in the Security Target, which specifies conformance to the Protection Profile for Application Software v1.2; April 22, 2016. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished on September 27, 2019.

# 9. VALIDATOR COMMENTS/RECOMMENDATIONS

As stated earlier in this report, the product is the CyberArk PAS Solution, which enables organizations to secure, provision, control, and monitor all activities associated with the privileged identities used in enterprise systems. PAS contains multiple applications that work together to provide privileged access security. However, the components of the PAS Solution were not evaluated as a distributed TOE but as standalone TOEs that work together. There are separate security targets, detailed test reports, assurance activity reports, and secure configure guidance supplement. This validation report covers the evaluation of the Enterprise Password Vault.

The reader should review the Guidance Documentation Supplements and the associated guidance documents identified in section 6 carefully to ensure secure configuration of the product.

All other items and scope issues have been sufficiently addressed elsewhere in the document

# 10. ANNEXES

*None*

# 11. SECURITY TARGET

CyberArk Software Ltd. Privileged Access Security – Digital Vault Server including Enterprise Password Vault (EPV) v10.4 Security Target, version 0.17, September 25, 2019

# 12. GLOSSARY

- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

# 13. BIBLIOGRAPHY

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012.
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012 .
4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012.
5. Protection Profile for Application Software v1.2; April 25, 2016
6. CyberArk Software Ltd. Privileged Access Security – Digital Vault Server including Enterprise Password Vault (EPV) v10.4 Security Target, version 0.17, September 25, 2019
7. Assurance Activity Report for CyberArk Software Ltd. Privileged Access Security – Digital Vault Server including Enterprise Password Vault (EPV) v10.4, version 1.0, September 2019
8. CyberArk Privileged Account Security - Digital Vault Server Including Enterprise Password Vault (EPV) v10.4 Evaluation Technical Report, version 0.2, September 25, 2019
9. PAS-Enterprise Password Vault (EPV) Version 10.4 Evaluation Detailed Test Report Version 0.5, September 27, 2019
10. CyberArk Software Ltd.; Privileged Access Security Enterprise Password Vault Architecture v10.4; Guidance Documentation Supplement; Version: 0.8
11. CyberArk: Privileged Access Security Installation Guide; Version 10.4
12. CyberArk: Privileged Access Security System Requirements; Version 10.4
13. CyberArk; Privileged Access Security End-user Guide; Version 10.4
14. CyberArk; Privileged Access Security Reference Guide; Version 10.4
15. CyberArk; Privileged Access Security Implementation Guide; Version 10.4