Agenzia per la Cybersicurezza Nazionale

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti
ISO/IEC 15408 Common Criteria (CC) CC:2022 Release 1

Certificato n. *(Certificate No.)*	15/2026
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/CCL/16/2024/RC, v 1.0.
Decorrenza *(Date of 1st Issue)*	25 febbraio 2026
Nome e Versione del Prodotto *(Product Name and Version)*	Commvault Platform Release CPR2025E (11.42.41)
Sviluppatore *(Developer)*	Commvault Systems Inc.
Tipo di Prodotto *(Type of Product)*	Protezione dati (Data protection)
Livello di Garanzia *(Assurance Level)*	EAL2, conforme a CC Parte 3
Conformità a PP *(PP Conformance)*	Nessuna
Funzionalità di sicurezza *(Conformance of Functionality)*	TDS specifico per il prodotto, CC Parte 2 estesa

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR
(CCRA recognition for components up to EAL2 and ALC_FLR only)

Riconoscimento SOGIS MRA per componenti fino a EAL4
(SOGIS MRA recognition for components up to EAL4)

Roma, 25 febbraio 2026

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

[ORIGINAL SIGNED]

Il prodotto IT (*Information Technology*) identificato nel presente certificato è stato valutato presso un LVS (Laboratorio per la Valutazione della Sicurezza) accreditato e abilitato/approvato utilizzando la Metodologia Comune per la Valutazione di Sicurezza della Tecnologia dell'Informazione CEM:2022 revisione 1 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione CC:2022 revisione 1. Questo certificato si applica solo alla versione e al rilascio specifici del prodotto nella sua configurazione valutata e unitamente al Rapporto di certificazione completo. La valutazione è stata condotta in conformità alle disposizioni dello Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004) e le conclusioni dell'LVS nel Rapporto di Fine Valutazione sono coerenti con le evidenze addotte. Il presente Certificato non costituisce un sostegno o promozione del prodotto IT da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosca o dia effetto a questo certificato, e nessuna garanzia del prodotto IT, da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosce o dà effetto a questo certificato, è espressa o implicita.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using Common Methodology for Information Technology Security Evaluation CEM:2022 release 1 for conformance to *Common Criteria for Information Technology Security Evaluation CC:2022 release 1. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of the National scheme for the evaluation and certification of the security in the sector of information technology (Prime Ministerial Decree of 30 October 2003 - Official Journal no. 93 of 27 April 2004) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product, by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.*

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Commvault Platform Release CPR2025E (11.42.41)

OCSI/CERT/CCL/16/2024/CR

Version 1.0

25 February 2026

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	25/02/2026

2 Table of contents

3 Acronyms

3.1 National scheme

DPCM	Decreto del Presidente del Consiglio dei Ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Agreement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other acronyms

API	Application Program Interface
CVE	Common Vulnerabilities and Exposures
DDB	Deduplication Database
DR	Disaster Recovery
NTP	Network Time Protocol
XSS	Cross-site Scripting
VADP	VMware APIs for Data Protection
VM	Virtual Machine

VSA	Virtual Server Agent

4 References

4.1 Normative references and national Scheme documents

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, November 2022, CC:2022 Revision 1 CCMB-2022-11-001

[CC2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, November 2022, CC:2022 Revision 1 CCMB-2022-11-002

[CC3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, November 2022, CC:2022 Revision 1 CCMB-2022-11-003

[CC4] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, November 2022, CC:2022 Revision 1 CCMB-2022-11-004

[CC5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, November 2022, CC:2022 Revision 1 CCMB-2022-11-005

[CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2014

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, November 2022, CC:2022 Revision 1 CCMB-2022-11-006

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 agosto 2023

[NIS5] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 5/23 – Condizioni per lo svolgimento di test da remoto in valutazioni Common Criteria, versione 1.1, 21 agosto 2023

[SOGIS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3, January 2010

4.2 Technical documents

[ETRv3] “Evaluation of Commvault Platform Release CPR2025E (11.42.41)” Evaluation Technical Report, date 2026-02-20, Version 3, The Agile Cybersecurity Laboratory (Budapest site).

[ST] Security Target Commvault Platform Release CPR2025E (11.42.41) Evaluation Assurance Level (EAL): EAL2, Document Version: 1.9, Date: 2026-02-19 (PUBLIC)

[CPR2023E] Offline product documentation, “11.32_offlinedocs.zip”, v1.0
SHA256: 33a3355f140144a6bc79c5384b5f8481dd27923965247b9b0dd413973aac9cde

[CPR2025E] Offline product documentation, “11.42_offlinedocs.zip”, v1.0
SHA256: 2e54444fce28b16a6818ee4328cdc0afa96c1834e5c91d1d767dedf882cc762c

[AGD_v1.9] Guidance Document Commvault Platform Release CPR2025E (11.42.41) Evaluation Assurance Level (EAL): EAL2, version: v1.9, date: 2026-02-19
SHA-256: 6b9a0763a356096012499dfde7eddb3ceedb177c8fe3153ef5ac2540bc97f2c9

5 Recognition of the certificate

5.1 European recognition of CC certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT Products. A higher recognition level for evaluations beyond EAL4 is provided for IT Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under SOGIS-MRA for all claimed assurance components up to EAL4.

5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] was ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all claimed assurance components up to EAL2 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the product “**Commvault Platform Release CPR2025E (11.42.41)**”, developed by Commvault Systems Inc., which is an enterprise data backup and recovery software. The Commvault Platform CPR2025E implements the Intelligent Data Management features to backup different versions of the data, stores the data in a space efficient and encrypted format. The TOE is a software-based solution and there is no physical hardware which should be delivered to the customer.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3 and NIS5]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should also review the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC version CC:2022 Release 1 for the assurance level EAL2, according to the information provided in the Security Target [ST] and in the configuration shown in “Annex B - Evaluated configuration” of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3] e [CC5]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA], and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product "Commvault Platform Release CPR2025E (11.42.41)" to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should also review the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Commvault Platform Release CPR2025E (11.42.41)
Security Target	Security Target Commvault Platform Release CPR2025E (11.42.41) Evaluation Assurance Level (EAL): EAL2, Document Version: 1.9, Date: 2026-02-19 (PUBLIC)
Evaluation Assurance Level	EAL2
Developer	Commvault Systems Inc
Sponsor	Commvault Systems (Austria) Gmb
LVS	CCLab - The Agile Cybersecurity Laboratory (Budapest site).
CC version	CC:2022 Release 1
PP conformance claim	No conformance claimed
Evaluation starting date	11 December 2024
Evaluation ending date	20 February 2026

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled and in the configuration shown in "Annex B - Evaluated configuration" of this Certification Report.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description refer to the Security Target [ST].

The Target of Evaluation (TOE) is Commvault Platform Release CPR2025E (11.42.41), which is an enterprise data backup and recovery software. The Commvault Platform CPR2025E implements the Intelligent Data Management features to backup different versions of the data, stores the data in a space efficient and encrypted format. The TOE is a software-based solution and there is no physical hardware which should be delivered to the customer.

For a detailed description of the TOE, refer to sections 1.3 and 1.4 of the Security Target [ST].

7.3.1 TOE architecture

An example deployment of the TOE is shown in Figure 1 and the following TOE components can be seen:

- CommServe: It contains the central catalog and it is the main server. Users and configurations can be managed from here.
- Virtual Server Agent (VSA): A module that interacts with the hypervisor through the ESXI API to facilitate backup and recovery.
- MediaAgent: Behaves as data storage for the encrypted data. Physically it is the same virtual machine as the Commserve.

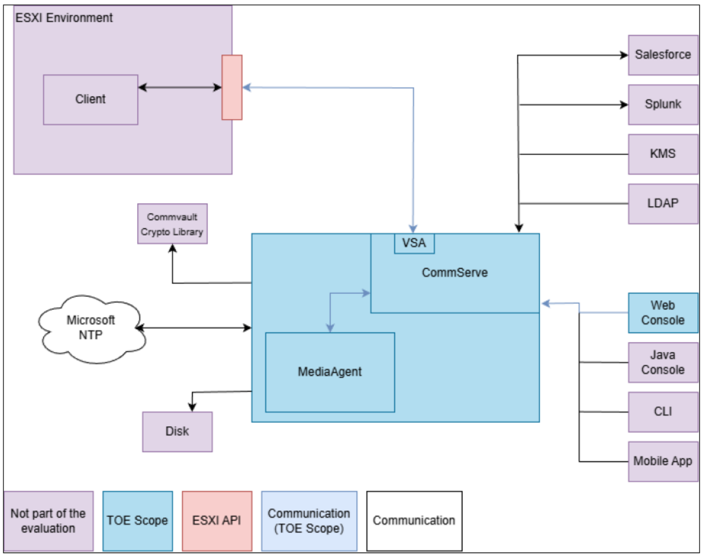

Figure 1 - TOE environment

The figure illustrates the TOE environment where the scope of the evaluation includes the CommServe Server where the management functions are available through the Command Center (Web Console), the MediaAgent, where the backup is saved on a virtual disk (physically the MediaAgent is the same as the CommServe server), the communication path between the components and the VSA module which interacts with the ESXI API.

The TOE needs a Client, not part of the TOE: a guest Windows Virtual machine running on ESX Server protected through the ESXI API.

Critical non-TOE component are:

- Client – It contains the customer data to be backed up. The Client, in this context is a virtual machine on an ESXI hypervisor environment. During the backup users can choose a single VM or a VM Group associated with the hypervisor environment. Choosing the VM Group will back up every VM associated to the group for the Hypervisor. The scope of the evaluation is backing up one virtual machine.
- Commvault Crypto Library 3.0 - Cryptographic module used for the cryptographic operations. TOE uses the Commvault Crypto Library for all cryptographic operations. It is a FIPS validated library.

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in section 3 of the Security Target [ST].

The TOE's major security features are the following:

- Data Transport from the source client to the storage facilitated by means of VSA - Backup operation.
- Data Transport from the storage to the client facilitated by means of VSA - Restore operation.
- Management interface - The Command Center (Web Console).
- Data Deduplication - DDBs (Deduplication database) may be defined as Deduplication Engines that achieves reduction of data across many different dependent Copies.
- Indexing of the Metadata for easy search and browse. - When in the backup phase the stream reaches the MediaAgent, the data is indexed and stored on the MediaAgent.
- Backup and Restore operation management (CommServe).
- System Disaster Recovery - By default, the CommServe software runs Disaster Recovery (DR) backup jobs to protect the CommServe production database.
- Network Topologies, Gateways, Throttling - Setting up an encrypted path between the TOE components on a specific tunnelling port.

The data deduplication, indexing of the metadata and disaster recovery are running in the background, there are no operations required on a management interface for them.

The TOE is further broken down into the security functions as follows:

- Security Audit: The TOE generates audit records for events associated with TSF-mediated actions, TOE startup, and TOE shutdown.
- User Data Protection: The TOE offers backup (offering DDB2) and restore capabilities to Backup Admin, managed through Plans.
- Identification and authentication: The TOE guarantees that access to TSF-mediated actions is restricted to authenticated and identified TOE users before any actions occur within the TOE.
- Security Management: The TOE offers management functionalities such as audit reviewing, encryption policy and key rotation policy management, backup plan management, backup data restoration, and local account management.
- Protection of the TSF: To ensure that the audit records have the correct time, the TOE is configured to synchronize with the Microsoft NTP servers, and the system time is used as a reliable timestamp.
- Trusted Path/Channels: Communication between the Command Center and CommServe is encrypted and trusted using TLSv1.2 compliant communication protocol.

A detailed description of the TOE security functionality is provided in section 7 of the Security Target [ST].

7.4 Documentation

The product's documentation ([CPR2023E], [CPR2025E]) and the [AGD_v1.9] document is sent to the customer via e-mail when receiving the license.

The documents can be verified using the corresponding SHA-256 hash string:

- Guidance document "Commvault Systems Inc. Guidance document Commvault Platform Release CPR2025E (11.42.41) Evaluation Assurance Level (EAL)", Version: v1.9 Release date: 2026-02-19

  SHA-256: 6b9a0763a356096012499dfde7eddb3ceedb177c8fe3153ef5ac2540bc97f2c9

- Product documentation ([CPR2023E]) "11.32_offlinedocs.zip"

  SHA-256: 33a3355f140144a6bc79c5384b5f8481dd27923965247b9b0dd413973aac9cde

- Product documentation ([CPR2025E]) "11.42_offlinedocs.zip"

  SHA-256: 2e54444fce28b16a6818ee4328cdc0afa96c1834e5c91d1d767dedf882cc762c

The documents contain all the information for secure initialization, configuration, and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in section 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] does not claim conformance to any Protection Profile (PP).

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3] and are from EAL 2 assurance package.

All the SFRs have been selected or derived by extension from CC Part 2 [CC2] (it includes FDP_BCK_EXT as extended component).

Security Target [ST] provides a complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that it constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab The Agile Cybersecurity Laboratory (Budapest site).

The evaluation was completed on 20 February 2026 with the issuance by LVS of the Evaluation Technical Report v3 [ETRv3], which was approved by the Certification Body on 23 February 2026. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in “Annex B - Evaluated configuration”.

Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; there is a probability, however small, that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to regularly check the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report v3 [ETRv3] issued by the LVS CCLab - The Agile Cybersecurity Laboratory (Budapest site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE “Commvault Platform Release CPR2025E (11.42.41)” meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL2, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in “Annex B - Evaluated configuration”.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL2.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	**Pass**
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	**Pass**
Security architecture description	ADV_ARC.1	Pass
Security-enforcing functional specification	ADV_FSP.2	Pass
Basic design	ADV_TDS.1	Pass
Guidance documents	**Class AGD**	**Pass**
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	**Pass**
Use of a CM system	ALC_CMC.2	Pass
Parts of the TOE CM coverage	ALC_CMS.2	Pass
Delivery procedures	ALC_DEL.1	Pass
Tests	**Class ATE**	**Pass**
Evidence of coverage	ATE_COV.1	Pass
Functional testing	ATE_FUN.1	Pass

Assurance classes and components		**Verdict**
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	**Pass**
Vulnerability analysis	AVA_VAN.2	Pass

Table 1 - Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in section 6 (Statement of Certification).

Potential customers of the product "Commvault Platform Release CPR2025E (11.42.41)" are suggested to properly understand the specific purpose of the certification by reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the "*Security Objectives for the Operational Environment*" specified in section 4 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all Assumptions described in section 3.3 of the Security Target [ST] shall be satisfied.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, "Annex A - Guidelines for the secure usage of the product" includes a number of recommendations relating to delivery, installation, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE (CC guidance [AGD_v.1.9]).

9 Annex A - Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE delivery

The following procedural steps define how the TOE is delivered to the customer:

Step	Delivery procedure description
1	The customer has to purchase a software as offered by Commvault first, and after the software is purchased a Commvault account is provisioned for the customer on store.commvault.com as well as support portal (support.commvault.com). Customers receive emails indicating their access enablement on support portal. There is no physical hardware which should be delivered to the customer.
2	The TOE binary is ready for download from the Commvault Store after logging in. The installer can be found in the Commvault Store under “Media Kits” > “LTS Media Kits”. The licence can be applied after the installation as described in [AGD_v1.9] section License Activation.
3	When clicking on the Download button there is an option to download for Linux or Windows versions. The customer downloads the installer of the certified TOE after identifying it based on the following parameters: Platform, File name, Size, SHA-256 checksum
4	After downloading the installer, the customer has to check the file’s integrity Size: 26.93 MB SHA-256 checksum: 16cc8c1043d3e83455c5b1ae585a78c083ca6f32425905cb23dd8f8215d4c0c1

Table 2 - Delivery procedure steps

9.2 Installation, configuration, and secure usage of the TOE

TOE installation, configuration and secure usage must be performed following the instructions contained in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the Common Criteria Guide [AGD_v1.9] contains detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure usage of the TOE in accordance with the security objectives specified in the Security Target [ST].

The product’s documentation ([CPR2023E], [CPR2025E]) and the [AGD_v1.9] document is sent to the customer via e-mail when receiving the license. In order to check the integrity of the document, you can follow the steps available in section 7.4 Documentation.

10 Annex B - Evaluated configuration

The Evaluators have deployed the TOE Commvault Platform Release CPR2025E (11.42.41) in a physical hardware that meets the following requirements:

- Windows Server 2019 x64
- CPU with at least 16 cores
- 32GB RAM
- 2 TB of working space for the CommServe database, the deduplication database (DDB), index, and job results

The Evaluators have installed also the operational environments components described in section 10.1.

The Evaluators have followed the [AGD_v1.9] document as a primary guidance document for the TOE installation and its functions.

10.1 TOE operational environment

The TOE operational environment consists of:

- Windows Server 2019 OS x64 (CPU with at least 16 cores, 32GB RAM, 2 TB of working space for the CommServe database, the deduplication database (DDB), index, and job results - SSD is recommended)
- MSSQL Server Database 2022
- Internet browser
- Commvault Crypto Library 3.0 (Installed along with the TOE)

In addition, an ESXI hypervisor environment where a Client VM (Windows Server 2019) is installed with the following requirements.

- vSphere, vCenter, vCenter Server Appliance, and ESX/ESXi: 4.1 or later, 5.0.x, 5.1.x, 5.5, 5.5.1, 5.5.2, 5.5.3, 5.5.6, 6.0, 6.0.1, 6.0.2, 6.0.3, 6.5, 6.7, 6.7.1, 6.7.2, 6.7.3, 7.x (all minor updates), 8.x (all minor updates).
- For any ESXi servers, the VMware vSphere Storage APIs - Data Protection or VADP[1].

[1] VADP is not available in the free version of ESXi. The Essentials licensing level or higher is required.

11 Annex C - Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities.

11.1 Test configuration

The Developer performed extensive tests to verify the functionality of the TOE. The tests cover all Subsystems, Modules and TSFIs of the TOE.
The Evaluators selected all the Developer provided tests for testing (100% coverage).

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer has performed extensive tests to verify the functionality of the TOE. The tests cover all TSFIs of the TOE.

The Developers organized the test cases the following way to cover all aspects of the TSF:

- Test Case 1: Security Audit
- Test Case 2: User Data Protection
- Test Case 3: Security Audit
- Test Case 4: Identification and Authentication
- Test Case 5: Security Management
- Test Case 6: Protection of the TSF
- Test Case 7: Trusted Path

11.2.2 Test coverage

The Evaluators have examined the test plan presented by the Developer and verified the complete coverage of the functional requirements (SFRs) and the TSFIs described in the functional specification. The Evaluators verified that the test cases are sufficient to demonstrate the internal behavior and the properties of the TSF.

11.2.3 Test results

The actual test results of all Developer's tests were consistent with the expected ones.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Test approach

In addition to the Developer's tests, the Evaluators created and performed 3 more independent test cases to test the TSF more in depth:

- Test Case 8: User Data Protection - the TOE is capable to perform backup and restore operations for valid users only
- Test Case 9: Identification and Authentication - the users have to be identified and authenticated before reaching any TSF function

- Test Case 10: Security Management - verify that each role is capable to perform an operation on the TOE only what associated with that role.

11.3.2 Test results

All Developer’s tests were run successfully and the Evaluators verified the correct behavior of the TSFIs and TSFs and correspondence between expected results and achieved results for each test.

All test cases devised by the Evaluators were passed successfully and the actual test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

The Evaluators conducted vulnerability analysis and penetration testing activities.

A search on public vulnerabilities on TOE and TOE components has been conducted. The analysis confirmed that there are no public vulnerabilities which were exploitable with the TOE evaluated configuration.

The Evaluators designed the following attack scenarios:

- Usernames guessing based on the responses from the TOE
- Undocumented user used to access TOE functions
- Endpoints accessible without authentication
- Role Privilege Escalation
- XSS Attacks

The Evaluators conducted penetration testing activities on the same instance of the TOE configured for functional and independent testing.

The Evaluators could then conclude that the TOE is resistant to a basic attack potential in its intended operating operational environment. No exploitable or residual vulnerabilities have been identified.