National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

HYCU for Enterprise Clouds

Report Number: CCEVS-VR-VID11409-2024
Dated: 1/17/2024
Version: 1.0

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

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Farid Ahmed

Lauren Brandt

Randy Heimann

Lisa Mitchell

Linda Morrison

Lori Sarem

Common Criteria Testing Laboratory

Furukh Siddique

Alexander Fannin

Shaunak Shah

Shaina Rae

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the HYCU for Enterprise Clouds Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in December 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended, and meets the assurance requirements of the *Collaborative Protection Profile for Network Devices*, Version 2.2e, 27 March 2020 [CPP_ND_V2.2E].

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory (CCTL) using the *Common Methodology for IT Security Evaluation* (Version 3.1, Rev. 5) for conformance to the *Common Criteria for IT Security Evaluation* (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the Protection Profile (PP). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

This TOE has been evaluated and certified by NIAP for use solely in the physical environments described in the Security Target. The deployment of this TOE into any cloud environment under the auspices of this certification is a violation of the terms of the NIAP Common Criteria Evaluation and Certification Scheme.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

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, security evaluations are conducted by commercial testing laboratories called CCTL. CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP.

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 Product Compliant 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.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	HYCU for Enterprise Clouds
Protection Profile	*Collaborative Protection Profile for Network Devices*, Version 2.2e, 27 March 2020 [CPP_ND_V2.2E]
Security Target	*HYCU for Enterprise Clouds Security Target*, Version 0.2.9, January 2024
Evaluation Technical Report	*Evaluation Technical Report for HYCU for Enterprise Clouds*, Version 0.6, 01/10/2024
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	HYCU Inc.
Developer	HYCU Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security 2400 Research Blvd. #395 Rockville, MD 20850
CCEVS Validators	Farid Ahmed, Lauren Brandt, Randy Heimann, Lisa Mitchell, Linda Morrison, Lori Sarem

3 Assumptions & Clarification of Scope

3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1 - Assumptions

ID	Assumption
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform. [TD0591 applied]
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).

ID	Assumption
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.VS_TRUSTED_ADMINISTRATOR	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
A.VS_REGULAR_UPDATES	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.VS_ISOLATION	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.

ID	Assumption
A.VS_CORRECT_CONFIGURATION	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

3.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the *Collaborative Protection Profile for Network Devices*, Version 2.2e, 27 March 2020 [CPP_ND_V2.2E].
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication, and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

4 Architectural Information

4.1 TOE Overview

The TOE is the HYCU, Inc. HYCU for Enterprise Clouds. HYCU for Enterprise Clouds provides application-consistent and virtualization-native data protection, data migration and disaster recovery. HYCU for Enterprise Clouds allows administrators to protect and manage clusters of a virtualized infrastructure with one integrated interface.

HYCU for Enterprise Clouds is a TOE that is installed as a virtual machine. The deployed virtual machine is accessed via a web GUI.

4.2 TOE Description

TOE is HYCU for Enterprise Clouds virtual appliance and management access, LDAP/S, SMTP and DNS. The NTP, storage and hypervisor are not included in TOE. For a full list see sections 7.1 and 7.2. The following diagram shows the environment and the evaluated TOE.

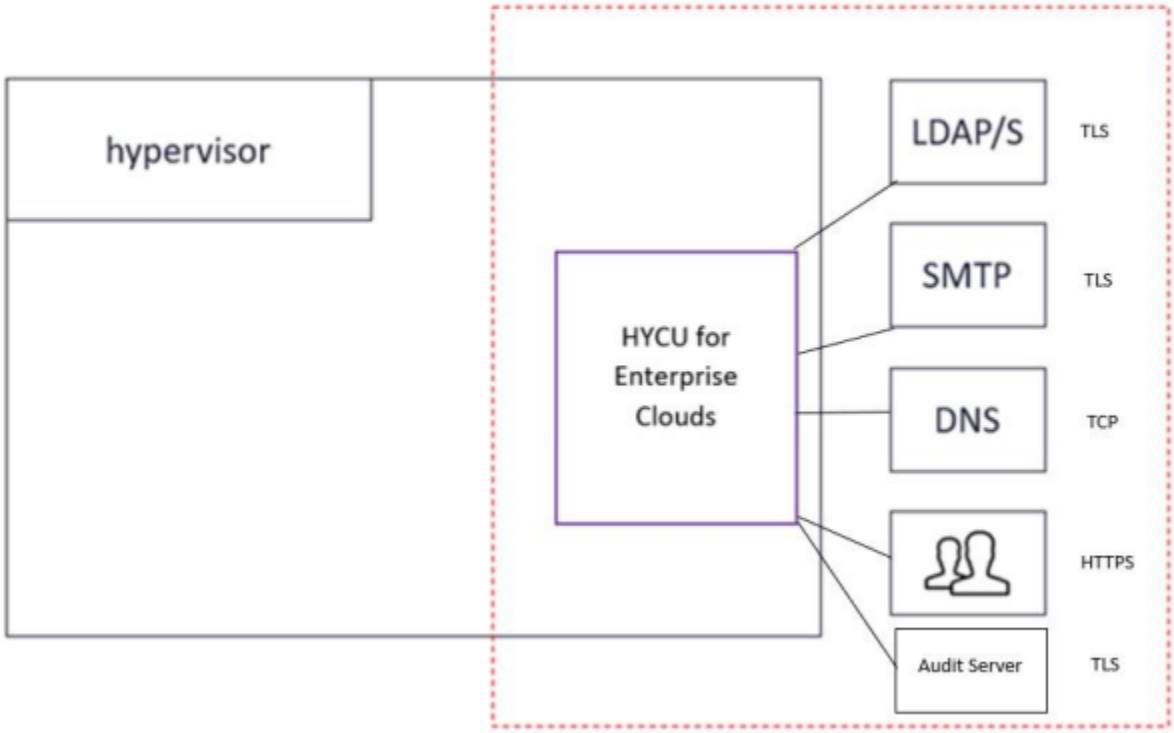

Figure 1 – Representative TOE Deployment

4.2.1 Physical Boundaries

The physical boundaries of the TOE are HYCU for Enterprise Clouds VM running on hypervisor and TOE hardware platform listed in section 7.1. The red dotted line is the evaluated configuration consisting of the HYCU for Enterprise Clouds (TOE) as well as all connections the

TOE makes externally (LDAP/S, SMTP/S, Audit Server). The HYCU for Enterprise Clouds is the only VM inside of the hypervisor.

5 Security Policy

5.1 Security Audit

The HYCU for Enterprise Clouds provides extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include:

- failure on invoking cryptographic functionality such as establishment, termination and failure of cryptographic session establishments and connections
- modifications to the group of users that are part of the Authorized Administrator roles
- all use of the user identification mechanism
- any use of the authentication mechanism
- administrator lockout due to excessive authentication failures
- any change in the configuration of the TOE
- changes to time
- initiation of TOE update
- indication of completion of TSF self-test
- maximum sessions being exceeded
- termination of a remote or local session
- attempts to unlock a termination session
- initiation and termination of a trusted channel
- failure of the trusted channel functions
- initiation and termination of a trusted path
- failure of the trusted channel path

The TOE is configured to transmit its audit messages to an external audit server. Communication with the audit server is protected using TLS and the TOE can determine when communication with the audit server fails. If that should occur, the TOE will store all audit records locally and when the connection to the remote audit server is restored, all stored audit records will be transmitted to the remote audit server.

The audit logs can be viewed on the TOE. The records include the date/time the event occurred, the event/type of event, the user associated with the event, and additional information of the event and its success and/or failure. The TOE does not have an interface to modify audit records.

5.2 Cryptographic Support

The TOE utilizes TLS (via HTTPS, SMTP/S and LDAPS) to securely communicate, both with external services (audit server, authentication server, mail server) and external clients (HTTPS for GUI administration). Both RSA and ECDSA keys are supported. Cryptographic support is restricted to the approved set of algorithms using a combination of system-wide policies and application-specific configuration. Random bit generation is served by underlying OS facilities (/dev/random).

5.3 Identification and Authentication

The TOE allows the Administrator to securely login to the management interface using a username and password. Usernames and passwords can be managed within the TOE or delegated to an external authentication server (AD/LDAPS). A lockout period protects against repeated authentication failures. The TOE can be configured with a custom login banner.

The private key and certificate for the TLS server can be imported or generated on the TOE. The TOE can issue a certificate signing request to be signed by an external certificate authority and then imported for use by the TLS server.

Trusted roots can be imported to establish trust with external servers. The TOE validates certificates of external servers – invalid or untrusted certificates result in rejected communication attempt. Online Certificate Status Protocol can be used to manage revocation.

5.4 Security Management

The TOE is managed remotely via a web user interface. Some functionality requires local console access. Roles and groups (tenants) can be defined and the roles can be assigned to users. TOE management is scoped within a built-in “Infrastructure group”. The TOE restricts configuration of security-related functions to the Administrator role of the Infrastructure group.

The Administrator is able to perform the following security-related functions:

- start and stop services
- update the TOE
- modify the behavior of the transmission of audit data to an external IT entity
- manage the cryptographic keys
- configure the cryptographic functionality
- set the time which is used for time-stamps
- manage the TOE's trust store and designate X509.v3 certificates as trust anchors
- import X.509v3 certificates to the TOE's trust store
- configure the session inactivity time before session termination or locking
- ability to configure the authentication failure parameters for FIA_AFL.1
- ability to configure access banner
- ability to update the TOE, and to verify the updates using hash comparison capability prior to installing those updates
- ability to administer the TOE locally and remotely

5.5 Protection of the TSF

Passwords of TOE-managed users are stored in a non-reversible encoding in the internal database. Private keys and passwords for external services are stored in an encrypted form within the TOE database. Password input is obscured by default (password reveal is optional).

The administrator can set the local TOE time using the console.

The TOE performs power-on self-tests to verify the integrity of the primary application server and supporting components. Self-tests can be performed on-demand.

The TOE has an update mechanism. Before performing updates, the administrator should manually validate the update image using the published hash available via HTTPS.

5.6 TOE Access

Idle sessions are terminated by the TOE after a configurable period of inactivity. In the web user interface, a short time before the inactivity period expires, a dialog is shown to notify of the impending session termination. The TOE lets the user sign out of their session on demand using a dedicated sign-out button (for web user interface) or the user can terminate the current shell (for the console).

The TOE can be configured with a custom login banner, for both the web user interface and the console.

5.7 Trusted Path/Channels

The TOE uses TLS to securely communicate with the following authorized IT entities:

- authentication server (Active Directory via LDAP/S)
- mail server (via SMTP/S)
- audit server (via HTTPS webhooks)

Administrator access to the web user interface is protected using TLS (via HTTPS).

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- *Common Criteria Guide: HYCU Data Protection for Enterprise Clouds Administrative Guide*, December 2023
- *HYCU Data Protection for Enterprise Clouds User Guide*, Version 4.5.1, July 2022

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The following environmental components are required to operate the TOE in the evaluated configuration:

Table 2 – Required Environmental Components

Component	Required	Purpose/Description
Lenovo ThinkSystem SR630, Xeon Silver 4208	Yes	TOE hardware platform
VMware ESXi 7	Yes	Hypervisor
LDAP/S	Yes	Remote authentication
SMTP	Yes	Notifications
Administrator Workstation	Yes	Management of the TOE
DNS server	Yes	Name resolution
Audit Server	Yes	Audit Log Transfer

7.2 Excluded Functionality

The following product functionality is not included in the CC evaluation:

- Linux and Windows based targets (NFS/CIFS)
- Cloud-based targets (Google, Amazon, Azure)
- iSCSI targets
- File-level recovery
- Reporting
- Nutanix File Server Backup
- VMware Virtual Machine Backup and Physical Machine Backup
- Virtual Machine Backup for Nutanix (AHV and ESXi)
- Application Awareness and Backup (Microsoft Active Directory, Exchange, SQL Server, Oracle Database)
- SSH
- Mutually authenticated TLS
- Encrypted backups
- S3 Compatible Targets
- NTP time synchronization
- Web GUI certificate authentication

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the proprietary detailed Test Report, and is summarized in the publicly available AAR.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the *Collaborative Protection Profile for Network Devices*, Version 2.2e, 27 March 2020 [CPP_ND_V2.2E]. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the ETR. The reader of this document can assume that all activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 Rev. 5 and CEM version 3.1 Rev. 5. The evaluation determined the TOE Name to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the HYCU for Enterprise Clouds that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the *Collaborative Protection Profile for Network Devices*, Version 2.2e, 27 March 2020 [CPP_ND_V2.2E].

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the *Collaborative Protection Profile for Network Devices*, Version 2.2e, 27 March 2020 [CPP_ND_V2.2E] related to the examination of the information contained in the TOE Summary Specification.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the

evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the *Collaborative Protection Profile for Network Devices*, Version 2.2e, 27 March 2020 [CPP_ND_V2.2E] related to the examination of the information contained in the operational guidance documents.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the *Collaborative Protection Profile for Network Devices*, Version 2.2e, 27 March 2020 [CPP_ND_V2.2E] and recorded the results in a Test Report, summarized in the ETR and AAR.

The validation team reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Common Criteria Guide: HYCU Data Protection for Enterprise Clouds Administrative Guide*, December 2023. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

This TOE has been evaluated and certified by NIAP for use solely in the physical environments described in the Security Target. The deployment of this TOE into any cloud environment under the auspices of this certification is a violation of the terms of the NIAP Common Criteria Evaluation and Certification Scheme.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as: *HYCU for Enterprise Clouds Security Target*, Version 0.2.9, January 2024.

13 Glossary

The following definitions are used throughout this document:

- **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.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **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 PP against the Common Criteria using the CEM 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.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **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.
- **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.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. *Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model*, Version 3.1 Revision 5.
2. *Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements*, Version 3.1 Revision 5.
3. *Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements*, Version 3.1 Revision 5.
4. *Common Evaluation Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 5.
5. *Evaluation Technical Report for HYCU for Enterprise Clouds*, Version 0.6, -1/10/2024.
6. *Common Criteria Guide: HYCU Data Protection for Enterprise Clouds Administrative Guide*, December 2023
7. *HYCU Data Protection for Enterprise Clouds User Guide*, Version 4.5.1, July 2022
8. *Collaborative Protection Profile for Network Devices*, Version 2.2e, 27 March 2020.
9. *HYCU for Enterprise Clouds Security Target*, Version 0.2.9, January 2024.
10. *Test Plan for a Target of Evaluation*, Version 1.2, January 10, 2024.
11. *Assurance Activity Report for HYCU for Enterprise Clouds*, Version 0.9, January 2024.
12. *Vulnerability Assessment for HYCU v4.5.1*, Version 1.4, January 10, 2024.