National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Enveil ZeroReveal® Compute Fabric Server v4.6.3, Version 1.3

Report Number: CCEVS-VR-VID11432-2024
Dated: 05/24/2024
Version: 1.3

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 George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Fernado Guzman

Marybeth Panock

Jerome Myers

Swapna Katikaneni

Common Criteria Testing Laboratory

Eric Isaac

Rupal Gupta

Yogita Kore

Joan Marshall

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 Enveil ZeroReveal® Compute Fabric Server v4.6.3 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 May 2024. 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 Conformant, and meets the assurance requirements of the *Protection Profile for Application Software*, Version 1.4, 07 October 2021 and the *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019.

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory 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.

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 Common Criteria Testing Laboratories (CCTLs). 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	Enveil ZeroReveal® Compute Fabric Server v4.6.3
Protection Profile	Protection Profile for Application Software, Version 1.4, 07 October 2021 and Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019
Security Target	Enveil ZeroReveal® Compute Fabric Server v4.6.3 Security Target version 2.1
Evaluation Technical Report	Evaluation Technical Report for Enveil ZeroReveal® Compute Fabric Server v4.6.3
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Enveil, Inc.
Developer	Enveil, Inc
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Fernado Guzman Marybeth Panock Jerome Myers Swapna Katikaneni

3 Architectural Information

3.1 TOE Overview

The TOE is the Enveil ZeroReveal Compute Fabric Server (otherwise referred to as the ZeroReveal Server, or the TOE) software application which communicates to one or more instances of the Enveil ZeroReveal Compute Fabric Client software application via REST over mutually authenticated HTTPS over TLS.

The TOE is a homomorphic encryption engine for database queries. In normal database operation, a query is submitted in plain text, and a plain text answer retrieved for the querier. While the communication between the querier and the database engine itself may be transmitted through a tunnel such as IPsec, TLS, or SSH, the contents of the query are always in plaintext. The ZeroReveal Compute Fabric Client (evaluated separately) takes an authenticated user's database query and encrypts it using Enveil's proprietary homomorphic encryption process. This encrypted query is passed via a mutually authenticated TLS trusted channel from ZeroReveal Client to ZeroReveal Server. The encrypted query is never decrypted during this process, which prevents ZeroReveal Server and its owners/administrators from being able to tell what the query was searching for and what items in the database (if any) matched the query. The output of this process is an encrypted response that is sent back to ZeroReveal Client. In this way, the database itself is not strictly aware of what the query was and no individual point in the chain between the user and the information know what was requested.

The ZeroReveal Server (the TOE) and ZeroReveal Client are evaluated as software applications only and the homomorphic encryption techniques used for the ZeroReveal Client and ZeroReveal Server operations are outside the scope this evaluation.

The diagram below shows the parts of the TOE application, and how the evaluation security boundary is identified.

3.2 TOE Description

3.2.1 Evaluated Configuration

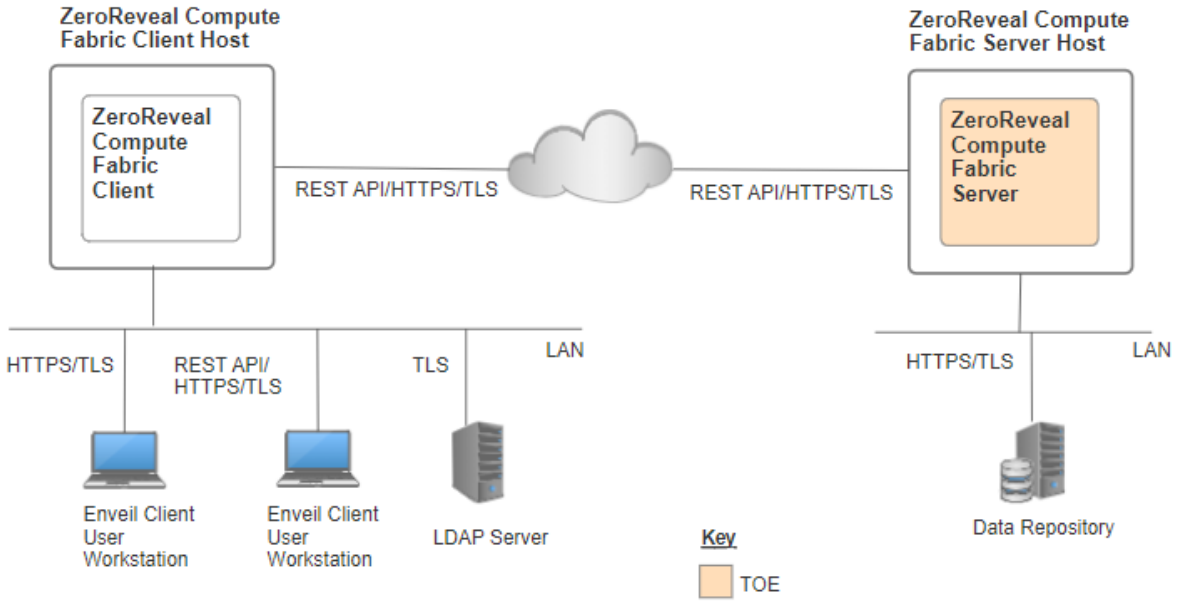
The TOE has been evaluated on the following host platform:

Rocky Linux 8.7 with SELinux on Intel Core i7-10710U (Comet Lake)

3.2.2 Physical Boundaries

The diagram below depicts a representative TOE deployment.

Figure 1: Representative TOE Deployment



The following items are required for the operational environment.

Table 1: Hardware and Software Environmental Components

Components	Mandatory/ Optional	Description
Hardware		
Enveil ZeroReveal® Compute Fabric Server v4.6.3 Host	Mandatory	The hardware running the TOE. The Server platform must include OpenJDK 8 JRE and Rocky Linux 8.7 with SELinux operating system installed.
Local Access	Mandatory	Local access to the ZeroReveal Server platform that enables an administrator to modify configuration files using a text editor and read log files. Access is via the local keyboard.
Enveil ZeroReveal® Compute Fabric Client v4.6.3 software and host platform	Mandatory	The Enveil ZeroReveal Client application which communicates with the ZeroReveal Server to process data queries. The TOE communicates with the ZeroReveal Client by receiving REST API commands sent using HTTPS over TLS.
Remote Data Repository	Mandatory	A remotely installed and configured database containing information against which ZeroReveal queries are executed. The TOE communicates with the remote database using HTTPS over TLS.
Software		
Rocky Linux 8.7 with SELinux OS	Mandatory	The operating system installed on the TOE's host.
OpenJDK 8	Mandatory	Java Platform that includes the Java Runtime Environment (JRE) installed on the TOE's host.

The TOE is the ZeroReveal Compute Fabric Server software that includes the following libraries:

- Java JSSE Library 8
- Bouncy Castle FIPS Provider v1.0.2.3
- Bouncy Castle FIPS TLS Provider v1.0.12.3
- GMP Library v6.2.0
- SEAL Homomorphic Encryption Library v3.7.2.0

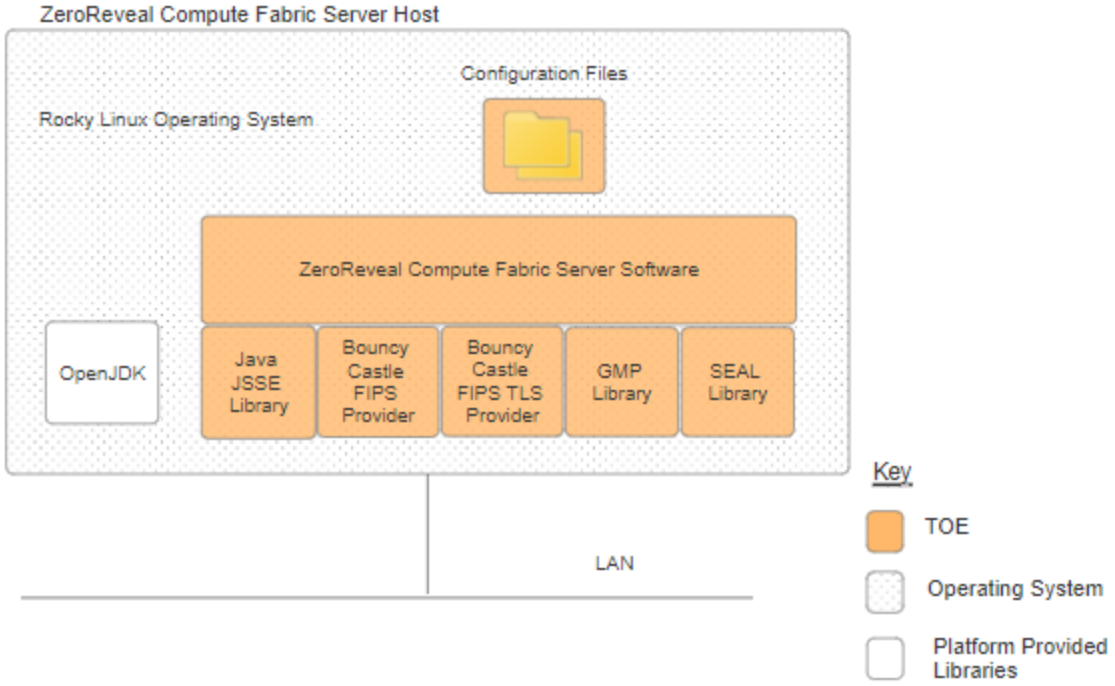
Additionally, the TOE boundary includes configuration files that include key strings that must be completed to configure the TOE in the evaluated configuration. The configuration files are modified by administrators and are accessed using the local keyboard.

The TOE's operational environment requires the TOE platform to have:

- Rocky Linux 8.7 with SELinux installed and running and
- OpenJDK 8 JRE installed.

The following diagram depicts the TOE and the Operational Environment of the ZeroReveal Compute Fabric Server Host.

Figure 2: ZeroReveal Server Host



4 Security Policy

4.1 Logical Boundaries

The TOE provides the security functionality required by the *Protection Profile for Application Software*, Version 1.4 and the *Functional Package for Transport Layer Security (TLS)*, Version 1.1.

4.2 Cryptographic Support

The cryptographic services provided by the TOE are described below.

Cryptographic Method	Use within the TOE
AES-GCM	TLS encryption
ECDSA	TLS key generation, signature generation and verification
RSA	TLS key generation, signature generation and verification
HMAC	Message integrity and authentication for TLS
AES-CCM	Storage of credentials
DRBG	Random bit generation for all cryptographic functions

Table 3 TOE Provided Cryptography

Each of these cryptographic algorithms have been validated for conformance to the requirements specified in their respective standards, as identified below.

Algorithm	Standard	Mode/Keysize	CAVP Cert. #
Cryptographic Asymmetric Key Generation (FCS_CKM.1/AK)			
RSA KeyGen	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3	2048 and 3072 bits	A4651
ECDSA KeyGen	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4	Curves P-256 and P-384	A4651
Cryptographic Key Establishment (FCS_CKM.2)			
ECDH Key Establishment	NIST SP 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"	Curves P-256 and P-384	A4651
Cryptographic Operation – Hashing (FCS_COP.1/Hash)			
SHA2-256	FIPS Pub 180-4	Digest size 256 bits	A4651
SHA2-384	FIPS Pub 180-4	Digest size 384 bits	A4651
SHA2-512	FIPS Pub 180-4	Digest size 512 bits	A4651
Cryptographic Operation - Keyed-Hash Message Authentication (FCS_COP.1/KeyedHash)			

Algorithm	Standard	Mode/Keysize	CAVP Cert. #
HMAC-SHA2-256	FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code' and FIPS Pub 180-4 'Secure Hash Standard'	Key size 256 bits, block size 512 bits, digest size 256 bits	A4651
HMAC-SHA2-384		Key size 384 bits, block size 1024 bits, digest size 384 bits	A4651
HMAC-SHA-512		Key size 512 bits, block size 1024 bits, digest size 512 bits	A4651
Cryptographic Operation – Signing (FCS_COP.1/Sig)			
RSA Digital Signature Algorithm (rDSA)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.	2048-bit and 3072 bits or greater	A4651
ECDSA schemes	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6.	P-256 and P-384 curves	A4651
SKC Cryptographic Operation – Encryption/Decryption (FCS_COP.1/SKC)			
AES-CCM	NIST SP 800-38C	256 bits	A4651
AES-CCM	NIST SP 800-38D	256 bits	A4651
Random Bit Generation from Application (FCS_RBG_EXT.2)			
HMAC_DRBG	NIST SP 800-90A	SHA2-512	A4651

Table 4 CAVP Algorithm Testing References

4.3 User Data Protection

The ZeroReveal Server network communication is restricted to user-initiated communication for responses to API requests from ZeroReveal Clients and accessing the remote database using TLS. Credentials are stored locally, encrypted using AES algorithm in CCM mode.

4.4 Identification and Authentication

The ZeroReveal server performs X.509v3 certificate validation functions to authenticate the certificate(s) during the establishment of the TLS trusted channels.

4.5 Security Management

Administrators manages the TOE via configuration files on each installation platform. The access interface and file editor used to modify the files is outside the scope of the TOE.

The TOE does not include any predefined or default credentials and utilizes the platform recommended storage process for configuration files.

4.6 Privacy

The TOE does not collect or transmit Personally Identifiable Information (PII) over the network.

4.7 Protection of the TSF

The TOE leverages platform provided package management for secure installation and updates. The TOE installation package includes only those third-party libraries necessary for its intended operation. The TOE utilizes compiler-provided anti-exploitation capabilities.

4.8 Trusted Path/Channels

The TOE communicates to the ZeroReveal® Compute Fabric Client via REST API over mutually authenticated HTTPS over TLS and stores data in a remote database using TLS. Administrators configure the TOE via local access only, making changes to configuration files.

5 Assumptions, Threats & Clarification of Scope

5.1 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.

The following assumptions are drawn directly from the [AppPP].

ID	Assumption
A.PLATFORM	The TOE relies upon a trustworthy computing platform with a reliable time clock 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 in compliance with the applied enterprise security policy.

Table 5 Assumptions

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

ID	Threat
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.

Table 6 Threats

5.3 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 *Protection Profile for Application Software*, Version 1.4, 07 October 2021 and the *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019.
- 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.
- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The TOE consists solely of software and relies on its operational environment for supporting security functionality, as identified in the security target.
- The following functionality is explicitly excluded from the scope of evaluation; it was not evaluated during the common criteria evaluation, and no claims are made regarding the applicability, suitability, or functionality of the following TOE functions:

    - The homomorphic encryption process, including the algorithms, uses and the security strength of the resultant ciphertext.
    - The user interface to modify the local configuration files.

6 Documentation

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

- Enveil ZeroReveal® Compute Fabric Configuration Guide for Common Criteria v3.1, Version 4.6.3 [AGD].

To use the product in the evaluated configuration, the product must be configured as specified in this documentation.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE has been evaluated on the following host platform:

- Rocky Linux 8.7 OS on Intel Core i7-10710U (Comet Lake)

7.2 Excluded Functionality

The TOE is a software application, and as such many of the functions of the application itself are out of scope of a Common Criteria Evaluation. The following functionality is explicitly excluded from the scope of evaluation; it was not evaluated during the common criteria evaluation, and no claims are made regarding the applicability, suitability, or functionality of the following TOE functions:

- The homomorphic encryption process, including the algorithms, uses and the security strength of the resultant ciphertext.
- The user interface to modify the local configuration files.

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 following proprietary document:

- Test Plan and Report for Enveil ZeroReveal® Compute Fabric Server v4.6.3, v1.3, 07 May 2024[DTR]

A non-proprietary description of the tests performed and their results is provided in the following document:

- Assurance Activity Report for Enveil ZeroReveal® Compute Fabric Server v4.6.3, v0.7, 13 May 2024[AAR]

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to Protection Profile for Application Software, Version 1.4, 07 October 2021 [AppPP] and Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 [TLSPkg].

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in Protection Profile for Application Software. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

All testing was conducted at the Acumen Security offices located in 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from July 2023 through May 2024.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for Protection Profile for Application Software and Functional Package for Transport Layer Security were fulfilled.

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 *Protection Profile for Application Software*, Version 1.4, 07 October 2021 and the *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019.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 Enveil ZeroReveal® Compute Fabric Server v4.6.3 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 Enveil ZeroReveal® Compute Fabric Server v4.6.3 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 *Protection Profile for Application Software*, Version 1.4, 07 October 2021 and the *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019.

The validator 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 EAL 1 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 *Protection Profile for Application Software*, Version 1.4, 07 October 2021 and the *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019 related to the examination of the information contained in the TOE Summary Specification.

The validator 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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 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 *Protection Profile for Application Software*, Version 1.4, 07 October 2021 and the *Functional Package for Transport Layer Security (TLS),* Version 1.1, 01 March 2019 related to the examination of the information contained in the operational guidance documents.

The validator 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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator 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 EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the *Protection Profile for Application Software*, Version 1.4, 07 October 2021 and the *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019 and recorded the results in a Test Report, summarized in the ETR and AAR.

The validator reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the *Protection Profile for Application Software*, Version 1.4, 07 October 2021 and the *Functional Package for Transport Layer Security (TLS),* Version 1.1, 01 March 2019, 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 evaluator examined public domain vulnerability searches by performing a keyword search. The terms used for this search were based on the vendor's name, product name, and key platform features leveraged by the product. As a result, the evaluator performed a search using the following keywords:

- Enveil
- ZeroReveal Compute Fabric Server v4.6.3

- ZeroReveal
- Compute Fabric
- Rocky Linux 8.7
- Intel Core i7-10710U
- Java JSSE Library 8
- Bouncy Castle FIPS v1.0.2.3
- Bouncy Castle FIPS TLS v1.0.12.3
- GMP Library v6.2.0
- SEAL Homomorphic Encryption Library v3.7.2.0
- OpenJDK 8
- REST API
- TLS 1.2
- Oracle MySQL Server 8.0.32
- Third Party Libraries found in Appendix A of the ST

The last vulnerability search was performed on May 13, 2024. Any residual vulnerabilities applicable to the TOE were identified and mitigations were described.

The validator 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 addressed the vulnerability analysis Assurance Activities in the Protection Profile for Application Software, Version 1.4, 07 October 2021 [AppPP] and Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019 [TLSPkg], 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 performed the Assurance Activities in the *Protection Profile for Application Software*, Version 1.4, 07 October 2021 and the *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

As stated in section 5, the scope of this evaluation was limited to the functionality and assurances covered in the *Protection Profile for Application Software*, Version 1.4, 07 October 2021 and the *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the product needs to be assessed separately, and no further conclusions can be drawn about their effectiveness. The evaluated configuration is dependent upon the TOE being configured per the evaluated configuration described in section 7 and the instructions in the Administrator Guide document listed in section 6.

11 Annexes

Not applicable.

12 Security Target

• Enveil ZeroReveal® Compute Fabric Server v4.6.3 Security Target, v2.1, 11 April 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 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.
- **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. *Assurance Activity Report for Enveil ZeroReveal® Compute Fabric Server v4.6.3*, v0.7, 13 May 2024.
2. *Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model*, Version 3.1 Revision 5.
3. *Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements*, Version 3.1 Revision 5.
4. *Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements*, Version 3.1 Revision 5.
5. *Common Evaluation Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 5.
6. *Evaluation Technical Report for Enveil ZeroReveal® Compute Fabric Server v4.6.3*, v0.4, Aprill 11, 2024.
7. *Enveil ZeroReveal® Compute Fabric Configuration Guide for Common Criteria v3.1*, Version 4.6.3 [AGD].
8. *Enveil ZeroReveal® Compute Fabric Server v4.6.3 Security Target*, v2.1, 11 April 2024 [ST].
9. *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019 [TLSPkg].
10. *Protection Profile for Application Software*, Version 1.4, 07 October 2021 [AppPP].
11. *Assurance Activity Report for Enveil ZeroReveal® Compute Fabric Server v4.6.3, v0.7, 13 May 2024[AAR]*
12. *Test Plan for Enveil ZeroReveal® Compute Fabric Server, v4.6.3, Version 1.3, May 07, 2024[DTR]*.
13. *Vulnerability Assessment for Enveil ZeroReveal® Compute Fabric Server v4.6.3, v1.3, May 13, 2024.*