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.)*	03/2026
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/CCL/02/2025/RC, v1.0
Decorrenza *(Date of 1st Issue)*	23 gennaio 2026
Nome e Versione del Prodotto *(Product Name and Version)*	Everfox Data Guard v4.0.0.2
Sviluppatore *(Developer)*	Everfox LLC.
Tipo di Prodotto *(Type of Product)*	Dispositivi e sistemi di protezione perimetrale (Boundary Protection Devices and Systems)
Livello di Garanzia *(Assurance Level)*	EAL4+ (ALC_FLR.2) conforme a CC Parte 2 e Parte 3
Conformità a PP *(PP Conformance)*	Nessuna
Funzionalità di sicurezza *(Conformance of Functionality)*	TDS specifico per il prodotto conforme a CC Parte 2

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, 23 gennaio 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 versione 2022 revisione 1 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 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 version 2022 release 1 for conformance to *Common Criteria for Information Technology Security Evaluation version 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

Everfox Data Guard v4.0.0.2

OCSI/CERT/CCL/02/2025/RC

Version 1.0

23 January 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	23/01/2026

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 Programming Interface
CLI	Command Line Interface

COTS	Commercial Off The Shelf
DFM	Data Flow Manager
DFP	Data Filtering Process
EDG	Everfox Data Guard
FDG	ForcePoint Data Guard
INPA	Inbound Network Protocol Adapter
IP	Internet Protocol
ISO	Optical Disk Image
IT	Information Technology
NPA	Network Protocol Adapter
NTP	Network Time Protocol
ONPA	Outbound Network Protocol Adapter
OS	Operating System
RHEL	Red Hat Enterprise Linux
RW	Read/Write
RO	Read Only
SSH	Secure Shell
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

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

[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

[NIS4] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Gestione nel tempo delle garanzie di prodotti certificati, versione 1.1, 21 agosto 2023

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

4.2 Technical documents

[ADM_GUIDE] Everfox Data Guard (Formerly Forcepoint Data Guard) Version 4.0.0.2 Administrator’s Guide, 5 November 2024

[AGD] Everfox LLC Data Guard v4.0.0.2 Guidance document for Common Criteria, Guidance Documentation Supplement, Version 0.7, 15 October 2025

[ETR1] Evaluation of Everfox Data Guard v4.0.0.2, EVERFOX-026_ETR_v1, CCLab Software Laboratory, Version: v1, 28 October 2025

[ST] Everfox LLC Data Guard v4.0.0.2 Security Target, Version 0.9, 23 January 2026

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 named "**Everfox Data Guard v4.0.0.2**", developed by Everfox LLC.

The Target of Evaluation (TOE) is a software product designed to inspect, validate, and filter network traffic using a flexible rules engine that allows administrators to implement data protection and sharing policies for enterprise data. It runs on COTS hardware and is deployed between domains or networks of different security or classification levels. The TOE only includes the software application.

The TOE inspects and filters transiting data flows by applying the Lua[1] runtime filtering rules to the traffic that flows between the NPAs (Network Protocol Adapters). By default, no data can flow between the NPAs unless the rules allow the flow. Administrators use the administrative CLI to implement rules to define unidirectional or bidirectional flow. The rules are based on the Lua scripting language. Lua rules provide flexible filtering and data validation to allow or drop a data payload from a high-level (interface, network zone, or protocol) down to the byte level for deep content inspection.

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 and Scheme Information Notes [NIS1, NIS2, NIS3, NIS4]. 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 review also 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 EAL4, augmented with ALC_FLR.2 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]) 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.

[1] Lua (standing for moon) is a lightweight, high-level, multi-paradigm programming language designed mainly for embedded use in applications.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product named "Everfox Data Guard v4.0.0.2" 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	Everfox Data Guard v4.0.0.2
Security Target	Everfox LLC Data Guard v4.0.0.2 Security Target, Version 0.8, 2025-10-15 [ST]
Evaluation Assurance Level	EAL4, augmented with ALC_FLR.2
Developer	Everfox LLC
Sponsor	Corsec Security, Inc.
LVS	CCLab – The Agile Cybersecurity Laboratory (Debrecen site)
CC version	CC:2022 Release 1
PP conformance claim	No conformance claimed
Evaluation starting date	January 15, 2025
Evaluation ending date	October 28, 2025

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 it is possible to refer to the Security Target [ST].

The Target of Evaluation (TOE) is a is a software solution that runs on COTS hardware and is deployed between domains or networks of different security or classification levels. The TOE inspects and filters transiting data flows by applying the Lua runtime filtering rules to the traffic that flows between the NPAs (Network Protocol Adapters). By default, no data can flow between the NPAs unless the rules allow the flow.

Administrators use the administrative CLI to implement rules to define unidirectional or bidirectional flow. The rules are based on the Lua scripting language. Lua rules provide flexible filtering and data validation to allow or drop a data payload from a high-level (interface, network zone, or protocol) down to the byte level for deep content inspection.

The TOE generates audit records for configuration changes, successful CLI commands, flow events, and startup and shutdown of the audit function. An authorized administrator filters and views the audit records from the CLI.

An administrator can only access the TOE after the administrator is identified by the TOE and assigned the role associated with the logged in account.

For a detailed description of the TOE, users can refer to section 1.6 of the Security Target [ST].

7.3.1 TOE architecture

The TOE software is available as an ISO image that includes the EDG 4.0 application and all its components. The TOE is separated into the following components:

- *Data Flow Manager* (DFM)

  The DFM is the center point to create and monitor the filtering pipeline processes. Processes are created based on Data Flow definitions. The DFM starts the INPA, DFP, and ONPA processes and monitors the health and status of these processes. The DFM also provides a CLI to allow administrators control over the DFM and to set the configuration files for all the components.

  Administrators use the TOE's CLI to configure settings such as allowing traffic to sources and destinations, applying data flow policies, and to importing the filter rules used to inspect and validate the data flows. The TOE's CLI also provides data flow management and monitoring tools to manage the startup and shutdown of filter processing and retrieval of various data flow transfer and filter statistics.

- *Data Filtering Process* (DFP)

  The DFP provides the core filtering capabilities for the TOE. The DFP handles the input/output operations for the flow data and hosts the Filtering Engine. The Filtering Engine is a customized version of the Lua v5.1.5 runtime environment, which is embedded in the TOE's software. Administrators implement rule sets written in Lua's scripting language to validate the data flowing through the Filter Engine. The Filter Engine can be used to chain multiple DFP filters.

  The DFP receives data payloads from the INPA and applies filter rules to determine if the data should be passed or dropped. If the data passes validation, it is passed to the ONPA. The filter rules are constructed using Lua programming language on top of the TOE filter APIs.

- *Inbound Network Protocol Adapter* (INPA)

  The INPA receives traffic from the environment. The traffic originates from an external source endpoint over a UDP or TCP connection. The INPA extracts the data payload and checks the configured data flow policies before send any of the allowed data to the DFP for filtering. The configuration file for the INPA is updated by the DFM after a RW administrator makes changes from the CLI.

- *Outbound Network Protocol Adapter* (ONPA)

  The ONPA receives its data payload from the DFP and checks the configured data flow policies before sending the payload to an external destination endpoint using a UDP or TCP connection.

The configuration file for the ONPA is updated by the DFM after a RW administrator makes changes from the CLI.

The TOE runs on RHEL 8.10 OS (part of TOE environment), which in turn provides core services such as authentication, data storage, SSH (Secure RHEL Shell) for remote authentication, and TCP/IP networking support. The TOE runs on top of the RHEL platform using built-in modules and open-source components to provide enhanced security protection, including:

- SELinux type enforcement: Provides mandatory access control for higher assurance enforcement of process execution and separation. Access control to and from an external network is enforced based on the zone ID associated with an administrator-named zone.
- Iptables: Provides packet filtering capabilities to control inbound and outbound access to network services.

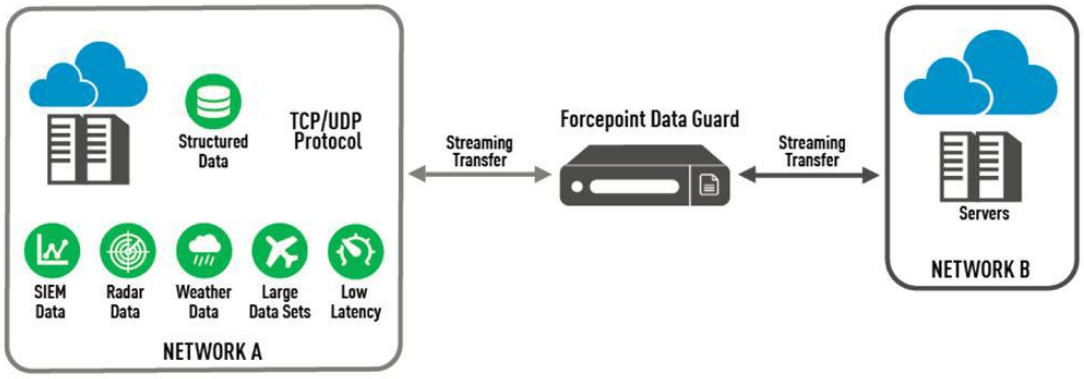

Figure 1 - TOE TCP/UDP Data Transfer Architecture

The following table specifies the minimum system requirements for the proper operation of the TOE.

Category	Requirement
Hardware	The minimum hardware requirements include the following: • At least one network interface card • 2 CPU • 2 GB of memory • 120 GB of storage
Networks	Inbound and outbound networks are required for the TOE to filter traffic.

Table 1 - TOE Minimum Requirements

TOE architecture and physical boundaries are illustrated in Figure 2.

The TOE is a software product which runs on a commercially available hardware server compliant with the minimum software and hardware requirements as listed in Table 1.

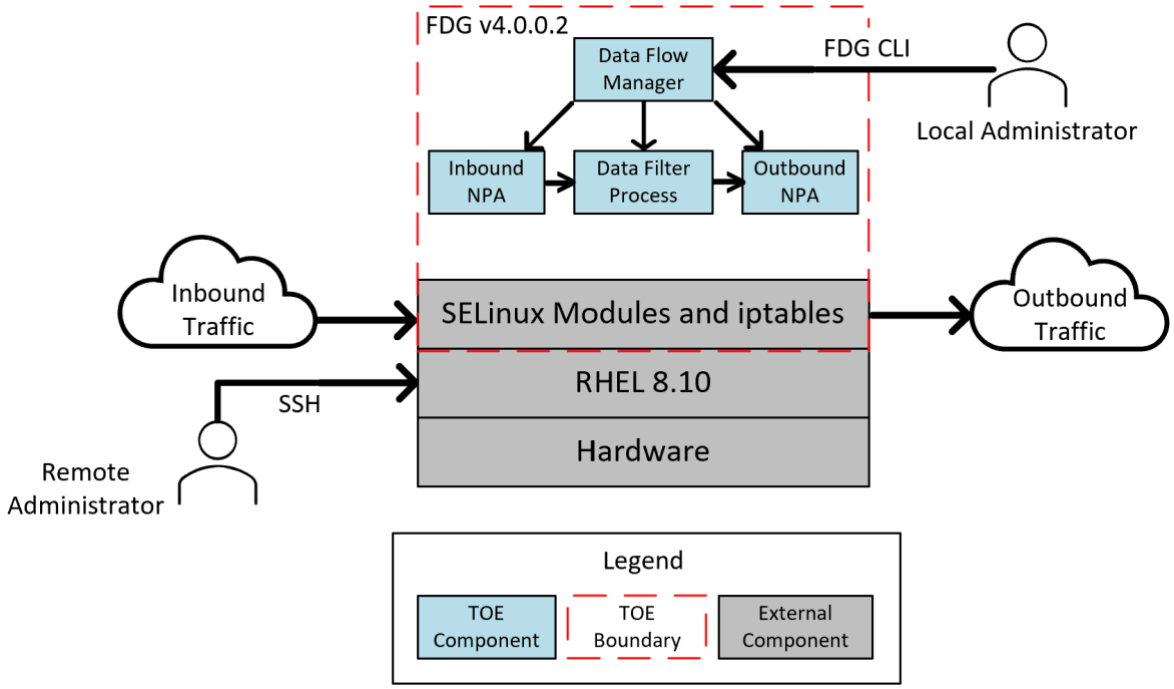

Figure 2 - Physical TOE Boundary

The TOE bridges communication between two separate external networks. The INPA receives network traffic from the external inbound network over a TCP or UDP connection and sends the traffic to the DFP for filtering. The ONPA receives the filtered data from the DFP and sends the data to the external outbound network over a TCP or UDP connection. Management of the TOE is performed via the CLI using either a remote SSH connection or the local console.

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].

For a detailed description of the TOE Security Functions, consult section 1.6.2 and Chapter 7 of the Security Target [ST]. The major security features are summarized in the following sections.

The SFRs implemented by the TOE are grouped under the following Security Function Classes:

- Security Audit
- User data protection
- Identification and authentication
- Security management

7.3.2.1 Security Audit

Audit functionality is provided by the TOE for generation of audit records for the startup/shutdown

of the audit function, configuration changes, and data flow events. From the TOE's CLI, administrators may view the following log files: audit.log, xguard-admin.log and xguard-flow.log.

7.3.2.2 User data protection

Information flow control is provided by the TOE with the INPA Information Flow SFP (INPA SFP), ONPA Information Flow SFP (ONPA SFP) and the Flow SFP. The INPA SFP controls the flow of inbound data from an external network. The ONPA SFP controls the flow of outbound data to an external network. The Flow SFP controls what is allowed to pass between the INPA and ONPA after filtering the data in the DFP. By default, no data is allowed to flow unless the flow is defined and permitted. A RW administrator defines the flow filtering rules using the Lua scripting language and imports the rules as a Lua file.

7.3.2.3 Identification and authentication

The TOE requires administrators to be identified by their TOE roles before gaining access to any TOE data or functionality.

7.3.2.4 Security management

The TOE provides the capability to manage the security functionality, TSF data, and security attributes of the TOE. The TOE also provides the read-only (RO) and read-write (RW) roles. The read-only role provides limited capabilities to view TSF data. The read-write role provides full administrative capabilities to manage the TSF. An administrator assigned to the RO role is referred to as a RO administrator. An administrator assigned to the RW role is referred to as a RW administrator. The unqualified term "administrator," when not preceded by RO or RW, refers to both RO administrators and RW administrators.

7.4 Documentation

The guidance documentation specified in "Annex A – Guidelines for the secure usage of the product" is delivered to the customer together with the product.

The guidance documentation contains 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 TOE does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3] and are from EAL4 assurance package, augmented with ALC_FLR.2 component.

All the SFRs have been selected from CC Part 2 [CC2].

It is possible to refer to the Security Target [ST] for the 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 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 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 (Debrecen site).

The evaluation was completed on October 28, 2025, with the issuance by the LVS of the approved Evaluation Technical Report [ETR1].

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 the TOE in the evaluated configuration corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report, with specific reference to section 8.2.

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 [ETR1] issued by the LVS CCLab – The Agile Cybersecurity Laboratory (Debrecen site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE named "Everfox Data Guard v4.0.0.2" meets the requirements of Part 2 and 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4 augmented with ALC_FLR.2 with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in "Annex B – Evaluated configuration".

Table 2 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 EAL4 augmented with ALC_FLR.2 (augmentation in *italics* in Table 2).

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
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Modular design	ADV_TDS.3	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
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass
Delivery procedures	ALC_DEL.1	Pass
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass

Assurance classes and components		Verdict
Well-defined development tools	ALC_TAT.1	Pass
Flaw reporting procedures	*ALC_FLR.2*	*Pass*
Test	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Focused vulnerability analysis	AVA_VAN.3	Pass

Table 2 - 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 "Everfox Data Guard v4.0.0.2" 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.

As mentioned in section 7.8, the Certification Body recommends reviewing the assumptions in the [ST], section 3.3, which are necessary conditions to be implemented for the TOE security:

- *A.ADMIN* - There are one or more competent individuals encharged to manage the TOE and the security of the information it contains. Administrators are trusted and assumed not to be willfully hostile to the TOE.
- *A.AUTHENTICATION* - The platform that the TOE is installed on will provide adequate authentication methods for TOE administrators.
- *A.PHYSICAL* - The TOE is located within a controlled access facility.
- *A.PROTECT* - The TOE software will be protected from unauthorized modification.
- *A.PLATFORM* - The TOE is installed on the appropriate, dedicated hardware and the platform contains only the approved applications needed to support the TOE as per the installation guidance.
- *A.NETCON* - The TOE environment provides network connectivity between the TOE and external networks.
- *A.TIMESTAMP* - The IT environment provides the TOE with the necessary and reliable timestamps.

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 ([ADM_GUIDE], [AGD]).

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

Everfox delivers their products to customers using digital distribution. All digital downloads are provided using Kiteworks links.

Product documentation and software will be available only to recipients of the email containing Kiteworks links. The Kiteworks links are temporary with a maximum of one week before they become invalid.

The TOE installation ISO, *fdg-4-0-0-2-38816-GA-2024-11-05.iso*, contains the TOE installation files, and the TOE documentation ISO *fdg-4-0-0-2_documentation_2024-11-05.iso* contains the TOE documentation files.

Checksum files are provided along with product ISO files. The Customer can check the integrity of the installation .ISO and the Documentation .ISO by performing SHA256 checksum and comparing it with the checksum files provided by Everfox and they should match. Customers should contact Everfox via email in order to obtain the TOE Guidance Supplement ([AGD]), delivered over Kiteworks. A license key must be obtained by the Customer in order to have a fully operational system, by contacting Everfox through multiple communication channels (web, e-mail, phone).

9.2 Installation, configuration and secure usage of the TOE

TOE installation, configuration and secure usage should be done by following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the documents [ADM_GUIDE] and [AGD] contain 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 items described in section 10.1 “TOE operational environment” must be available before performing the installation.

During the installation the administrator is prompted to set the default admin account password.

After installation, it is necessary to proceed with the steps in the “Logging In” section of [ADM_GUIDE] “Chapter 8. Working with FDG” to login with the default system administration account “admin”.

After logging in, the TOE software version can be verified via the CLI using the show version command available in Standard mode. The command should display version 4.0.0.2-38816. The TOE reference cannot be explicitly queried. When querying the TOE, "Forcepoint Data Guard v4.0.0.2" will be returned instead. The TOE was originally developed under the Forcepoint brand when the evaluation commenced and has not yet been fully rebranded in all components.

Once the version has been confirmed, enter Privileged Mode and then Configuration Mode following the steps in the “Privileged Mode” and “Configuration Mode” sections of [ADM_GUIDE] “Chapter 6. Using the Command-Line Interface (CLI)” respectively.

After entering Configuration Mode, it is requested to follow the steps in the “Adding an NTP Server” section of [ADM_GUIDE] “Chapter 8.5. Configuring the System Date, Time, and Timezone” to configure NTP.

While still in Configuration Mode, it is requested to follow the steps in the “Configuring Inbound Secure Shell (SSH)” section of [ADM_GUIDE] “Chapter 7. Configuring FDG” to configure the SSH connection. If needed, a new zone for the SSH connections has to be created following the steps in the “Configuring Zones” section.

To configure the network interface, it is requested follow the steps in the “Configuring Network Interfaces” section of [ADM_GUIDE] “Chapter 7. Configuring FDG” to assign the ethernet port to the required zone. Also, follow the steps in the “Configuring Network Routes” section. A hostname can be set to identify the server by following the steps in the “Configuring a Hostname” section.

A license file must be imported into the product to allow the flows. Follow the steps in the “Importing Files” section of [ADM_GUIDE] “Chapter 8. Working with FDG” to import the license file. Then follow the steps in the “Adding a License” section of “Chapter 7. Configuring FDG” to load the license file into FDG.

Now that the TOE is installed and connected to the external networks, the additional steps described in [AGD] section 3 must be taken to ensure the TOE is in its full CC-Evaluated Configuration.

10 Annex B – Evaluated configuration

The Evaluators followed the preparation steps defined in the [ADM_GUIDE] and [AGD] documents for the TOE being in the evaluated configuration.

The TOE is identified in the Security Target [ST] with the version number 4.0.0.2.

Refer to “Chapter 2: FDG Installation” of the [ADM_GUIDE] for instructions on installing the TOE.

10.1 TOE operational environment

The TOE operational environment includes the platform hardware, external networks, and TOE software as listed in Table 1. The platform hardware is installed such that it is only connected to the inbound and outbound external networks in the OE. An administrator configures the interfaces to the two external networks before the TOE is installed.

11 Annex C – Test activity

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

11.1 Test configuration

Testing activities have been carried out on the LVS premises.

The Evaluators verified the configuration of the test environment, including the TOE, and ensured that it was compliant with the AGD documentation [AGD] and the Security Target [ST].

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer used a manual testing approach. Different test cases were devised and performed to guarantee that each security function and aspect of the TSF was tested and verified.

11.2.2 Test coverage

The Evaluators have examined the test plan provided by the Developer and verified the coverage of the functional requirements (SFRs) and the TSFIs described in the functional specification. The tests cover all Subsystems, Modules and TSFIs of the TOE.

Namely, 5 Test cases were planned:

- TC ID.0 – Evaluated Configuration - This test case aimed at setting the TOE in the evaluated configuration
- TC ID.1 – Security Audit: This test aimed at demonstrating that the TOE generates audit records for startup and shutdown of the audit function.
- TC ID.2 – User Identification: The purpose of this test was to demonstrate that no TSF functionality is available to an administrator until the administrator is successfully identified by the TOE.
- TC ID.3 – User Data Protection: The purpose of this test case was to demonstrate that the TOE enforces the Input Network Interface Information, Output Network Interface Information, and Flow SFPs on inbound data traffic, outbound data traffic, and data flow between the Input Interface and Output Interface.
- TC ID.4 – Security Management: This test aimed at demonstrating that only an administrator with RW privileges may modify or delete.

The Evaluators verified that the test cases were sufficient to demonstrate the whole internal behaviour 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. All Developer's tests were run successfully, and the Evaluators verified the correct behaviour of the TSFIs and TSFs and the correspondence between expected results and achieved results for each test.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Test approach

In addition to the 5 Developer's test, the Evaluator created and performed 3 more independent test cases to test the TSF more in depth:

- EVERFOX-TEST01: verification that a disabled user cannot log in.
- EVERFOX-TEST02: verification that remote login is not possible unless it is configured.
- EVERFOX-TEST03: verification of addition of new users with all types of roles and their corresponding password change process.

11.3.2 Test results

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

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked with the TOE already used for the functional test activities, in the configuration of the TOE and the test environment already verified.

A search on public vulnerabilities on TOE and TOE components (e.g. OS) was conducted. The analysis confirmed that there were no public vulnerabilities exploitable with the TOE implementation and configuration.

Finally, the Evaluators conducted a methodical analysis of TOE documentation by the Developer to devise potential vulnerabilities to be verified and, if possible, exploited.

As result, the Evaluators could then conclude that the TOE is resistant to ENHANCED BASIC attack potential in its intended operating environment. No exploitable or residual vulnerabilities were identified.