Reference: 2024-37-INF-4721- v1	Created by: I007
Target: Limitada al expediente	Revised by: CALIDAD
Date: 23.02.2026	Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2024-37**
TOE	**CosmicGuard for Linux v2.2**
Applicant	**A83057034 - GMV SOLUCIONES GLOBALES INTERNET, S.A.U.**

References

[EXT-9116] Certification Request

[EXT-9940] Evaluation Technical Report

Certification report of the product CosmicGuard for Linux v2.2, as requested in [EXT-9116] dated 12/06/2024, and evaluated by SGS Brightsight Barcelona, S.L. (Unipersonal), as detailed in the Evaluation Technical Report [EXT-9116940] received on 18/12/2025.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product CosmicGuard for Linux v2.2.

The TOE is a software product designed to protect Linux endpoints (Agent) and managing the Access-Control-List (ACL) and the audit from a centralized web console (Server). The TOE employs this ACL to control the execution of applications within the endpoint and prevent any unauthorized access. This is achieved by enforcing the rules contained in this ACL.

The TOE provides security functionality, it includes functions such as Endpoint Protection, Management and Audit.

Developer/manufacturer: GMV SOLUCIONES GLOBALES INTERNET, S.A.U.

Sponsor: GMV SOLUCIONES GLOBALES INTERNET, S.A.U.

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: SGS Brightsight Barcelona, S.L. (Unipersonal).

Protection Profile: N/A.

Evaluation Level: Common Criteria 3.1 R5, EAL2.

Evaluation end date: 12/01/2026

Expiration Date[1]: 24/02/2031

All the assurance components required by the evaluation level EAL2 have been assigned a "PASS" verdict. Consequently, the laboratory SGS Brightsight Barcelona, S.L. (Unipersonal) assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product CosmicGuard for Linux v2.2, a positive resolution is proposed.

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

TOE SUMMARY

The TOE consists of three elements: the client, the server, which are the software CosmicGuard for Linux endpoints v2.2, and its accompanying documentation.

The TOE is comprised of these elements:

- The client consists of an agent that protects Linux endpoints by executing an ACL that prevents the execution of unwanted applications.
- The server consists of a centralized web management console for operating the solution and a platform that handles communications between the client and the server, called CosmicGuard Gateway, which is not a separate element but part of the server.
- The documentation needed for the installation and administration of the solution is provided in conjunction with the software.

The ACL can be built by a learning mechanism that automatically populates the rules or by including rules manually. It is recommended that this process be conducted in a test environment. Once the process is complete, the ACL can be sent to the target endpoint in the production environment, since then the rules will be applied immediately.

In terms of security, the features of the TOE are:

- Fine-grained control over process execution: The control implemented is based on blocking the execution of the processes which are not listed in the rules of the ACL and allowing its execution based on the path of the executable or its signature, in addition to the permissions with which it is launched and the parameters it executes.
- Control over loaded libraries: Access control to load libraries is restricted to those processes considered essential by the ACL rule, and only in read mode.
- File resources protection: File resource protection is based on restricting access to those files considered most critical only by those processes listed in the ACL rules in a number of modes, e.g. read/write, or read-only mode, etc…
- Control over inbound and outbound network connections: It is possible to restrict incoming and outgoing connections by basing the ACL rule on an IP address or a range of them, as well as a port or a range of them. Furthermore, it is possible to filter by protocol type, including TCP, UDP, or others.
- Centralized management console: Access to the console is web-based and via HTTPS connection, which allows centralized management of all the functionality of the solution, thus isolating the administration of the system.
- Identification and authentication of console users and role management: The user that accesses to the management web console is identified and authenticated. A wide range of roles can be assigned for the purpose of providing fine-grained control over the actions that can be performed on the console.

- Audit review of ACL violations: It is possible to determine the nature of the ACL violations at the endpoints.
- Audit of user actions: All actions performed by users within the administration web console are subject to audit for subsequent review.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2, according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ADV	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
ATE	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5:

- FAU_GEN.1(1): Audit data generation (EVENTS)
- FAU_GEN.1(2): Audit data generation (MGMT)
- FAU_GEN.2: User identity association
- FAU_SAR.1: Audit review
- FAU_SAR.2: Restricted audit review
- FDP_ACC.1(1): Subset access control (ENDPOINT)
- FDP_ACC.1(2): Subset access control (MGMT)
- FDP_ACF.1(1): Security attribute based access control (ENDPOINT)
- FDP_ACF.1(2): Security attribute based access control (MGMT)
- FDP_SDI.2: Stored data integrity monitoring and action
- FIA_AFL.1: Authentication failure handling
- FIA_SOS.1: Verification of secrets
- FIA_UAU.2: User authentication before any action
- FIA_UID.2: User identification before any action
- FMT_MSA.1(1): Management of security attributes (ENDPOINT)
- FMT_MSA.1(2): Management of security attributes (MGMT)
- FMT_MSA.3(1): Static attribute initialization (ENDPOINT)
- FMT_MSA.3(2): Static attribute initialization (MGMT)
- FMT_SMF.1: Specification of Management Functions
- FMT_SMR.1: Security roles
- FTA_SSL.2: User-initiated locking
- FTA_SSL.3: TSF-initiated termination

IDENTIFICATION

Product: CosmicGuard for Linux v2.2.

Security Target: *CosmicGuard for Linux. Security Target, version 7, 18/11/2025*.

Protection Profile: N/A.

Evaluation Level: Common Criteria 3.1 R5, EAL2.

SECURITY POLICIES

The use of the product CosmicGuard for Linux v2.2 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target, section 3.2 ("Organizational Security Policies").

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The detail of these assumptions is documented in the Security Target, section 3.3 ("Assumptions").

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product CosmicGuard for Linux v2.2, although the agents implementing attacks have the attack potential according to the AVA_VAN.2 of EAL2 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are those defined in the Security Target, section 3.1 ("Threats").

OPERATIONAL ENVIRONMENT FUNCTIONALITY

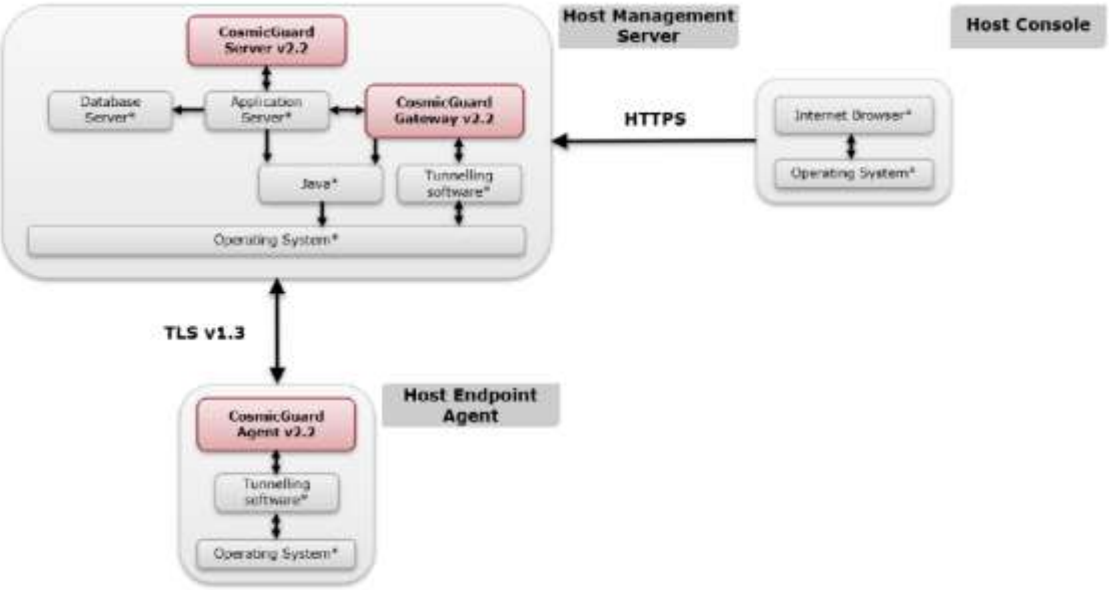
The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 4.2 ("Security Objectives for the Environment").

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE's general architecture is illustrated in the following figure:



Endpoint protection (agent)

The TOE offers the following features:

- Enforces the ACL in the endpoints, so that they are protected from executing unwanted or unknown applications. Authorization is granted based on defined rules:
    - Process execution: Restricts the execution of processes in the endpoint to those listed in the ACL.
    - Loaded libraries: Can restrict the loading of libraries in the endpoint to those listed in the ACL, if defined.
    - File resources protection: Restricts the access to resources in the endpoint to those listed in the ACL.
    - Inbound and outbound network connection: Restricts the establishment of inbound or outbound network connections to those listed in the ACL.
- Uses a mechanism of self-protection so that the ACL cannot be queried, nor modified, validating the integrity of the data.

Management (server)

The TOE Management Console offers the following functions:

- Provides access to the users through a centralized web console.
- Definition and management of the ACL.
- Requires users to be correctly identified and authenticated before executing any action.
- Handles the users and user roles from the management console.

Audit (agent and server)

The TOE offers the following audit functions:

- Generates events when a violation of the ACL occurs.
- Provides audit review for the violations of the ACL.
- Audits any actions performed by the management console users.

PHYSICAL ARCHITECTURE

The package that constitutes the TOE has the following cryptographic hash (SHA-256), which identifies it uniquely:

94119DE95A2E16A55C9FFF84F514D510C457250976FBB46385DEB4C5EACAAA5D

Inside the package, the following components will be found:

Host Management Server

- CosmicGuard Server v2.2 will be distributed as an EAR file.
- CosmicGuard Database scripts v2.2 will be distributed as an SQL script.
- CosmicGuard Gateway v2.2 will be distributed as a JAR file.

Host Endpoint Agent

- CosmicGuard Agent v2.2 will be distributed as a single compressed file (tar.gz) containing all the necessary for the installation.

Guidance

- CosmicGuard Installation Guide v2.2 [AGD_PRE] will be distributed as a PDF file.
- CosmicGuard User Guide v2.2 [AGD_OPE] will be distributed as a PDF file.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

[ST]	CosmicGuard for Linux. Security Target, version 7, 18/11/2025.
[AGD_PRE]	Installation Guide – CosmicGuard 2.2, version 6, 10/12/2025.
[AGD_OPE]	User Guide – CosmicGuard 2.2, version 7, 10/12/2025.

PRODUCT TESTING

Independent testing

The evaluator conducted independent testing using a representative sample of the developer's functional tests. The sample covers the 18% of the developer's tests and it was selected based on the following principles:

- Complete TSFI coverage, including those related to user authentication, access control, ACL management and audit generation.
- Representation of all major subsystems: CosmicGuard Agent and CosmicGuard Server.
- Inclusion of tests and its dependencies.
- Focus on security functionality.

As the developer testing covers all the TSFIs and all the SFRs, the strategy adopted by the evaluator for the independent testing considers the main functionalities that were not covered by the developer testing.

Penetration testing

A "Flaw hypothesis methodology" has been executed to assess the applicable potential vulnerabilities and devise a test plan. Common Criteria Methodology CEM v3.1 R5 has been used to rate the attacks.

The attacks executed cover 100% of the TSFI and focus in the known vulnerabilities and the common attacks.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product CosmicGuard for Linux v2.2 it is necessary the disposition of the following software components:

- Host Console:
    - Any hardware and operating system that supports the following:
        - Internet browser, Google Chrome 123.0.6312.59 (64-bits) or greater.
- Host Management Server:
    - Any hardware and operating system that supports the following:
        - Database Server, PostgreSQL 15.5.
        - Application Server, WildFly 26.
        - Java, OpenJDK 11.
        - Tunnelling Software, GhosTunnel 1.7.2 supporting TLS v1.3.
- Host Endpoint Agent:
    - Any hardware that supports the following:
        - Operating System, SLES 15 SP4.
        - Tunnelling Software, GhosTunnel 1.7.2 supporting TLS v1.3.
- All hosts can be executed in a virtual environment that meets the same requirements.
- Other services, such as NTP and PKI Infrastructure must be provided in the client's infrastructure.

Regarding the hardware components, the only requierement is that they shall support the software elements previously detailed.

Among all the possibilities offered by these software and hardware requirements, the configuration selected for the evaluation is the following:

- A virtual machine executed in Virtual Box 7.0.24 (recommended) with CosmicGuard Server v2.2 running on SLES 15 SP4 64-bits (Host Management Server).
- A virtual machine, executed in Virtual Box 7.0.24 (recommended) with CosmicGuard Agent for Linux v2.2 running on SLES 15 SP4 64-bits (Host Endpoint Agent).
- Access to the web console using Google Chrome 123.0.6312.59 (64-bits) or greater (Host Console) running on any compatible Operating System.
- All devices connected to the same LAN, remote access is not allowed.
- Virtual machines having the same time and date.

- Secure Boot must be enabled in the hypervisor used, recommended Virtual Box 7.0.16.
- Certificates must be issued by a trusted certification authority.
- The solution must be configured so that only Linux endpoints are managed, this can be achieved by following specific sections in the TOE User Guide [AGD_OPE].

EVALUATION RESULTS

The product CosmicGuard for Linux v2.2 has been evaluated against the Security Target *CosmicGuard for Linux. Security Target, version 7, 18/11/2025*.

All the assurance components required by the evaluation level EAL2 have been assigned a "PASS" verdict. Consequently, the laboratory SGS Brightsight Barcelona, S.L. (Unipersonal) assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL2, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

Aside on strictly follow the secure configuration guidance in **¡Error! No se encuentra el origen de la referencia.** and **¡Error! No se encuentra el origen de la referencia.**, no other recommendations were devised in this evaluation.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product CosmicGuard for Linux v2.2, a positive resolution is proposed.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

TSFI	TOE Security Functional Interface

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[ST] CosmicGuard for Linux. Security Target, version 7, 18/11/2025.

[AGD_PRE] Installation Guide – CosmicGuard 2.2, version 6, 10/12/2025.

[AGD_OPE] User Guide – CosmicGuard 2.2, version 7, 10/12/2025.

[ADV_ARC] Security Architecture – CosmicGuard for Linux v3.

[ADV_FSP] Functional Specification – CosmicGuard for Linux v4.

[ADV_TDS] TOE Design – CosmicGuard for Linux v3.

[ALC_CMC] CM Capabilities – CosmicGuard for Linux v4.

[ALC_CMS] Configuration Management Scope – CosmicGuard for Linux v6.

[ALC_DEL] Delivery Process – CosmicGuard for Linux v3.

[CI List] Configuration List from CosmicGuard for Linux (GMV) v1.

[ATE_COV] Testing Coverage – CosmicGuard for Linux v3.

[ATE_FUN] Functional Testing – CosmicGuard for Linux v3.

[AVA_OR_REPLY] Vulnerability Findings Report – CosmicGuard for Linux v1.

[AVA_FEEDBACK] Feedback to testbugs – CosmicGuard for Linux v1.

[ALC_PVS] Product Versioning Strategy – CosmicGuard for Linux v2.

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- *CosmicGuard for Linux. Security Target, version 7, 18/11/2025*.

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

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

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components selected.