MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

C112 Certification Report

CYSECA ENDPOINT APPLICATION CONTROL

File name: ISCB-5-RPT-C112-CR-v1
Version: v1
Date of document: 20 OCTOBER 2020
Document classification : PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.
T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999
www.cybersecurity.my

C112 Certification Report
CYSECA ENDPOINT APPLICATION CONTROL

20 OCTOBER 2020
ISCB Department

CyberSecurity Malaysia
Level 7, Tower 1,
Menara Cyber Axis, Jalan Impact,
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 7999 □ Fax: +603 8008 7000
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C112 Certification Report
DOCUMENT REFERENCE:	ISCB-3-RPT-C112-CR-v1
ISSUE:	v1
DATE:	20 OCTOBER 2020
DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 201601006881 (726630-U)

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 23rd Oct 2020, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme using the Common Methodology for IT Security Evaluation, version 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	8 October 2020	All	Initial draft
v1	20 October 2020	All	Final version

Executive Summary

The Target of Evaluation (TOE) is CYSECA Endpoint Application Control which consists of CYSECA Endpoint Application Control Server v1.2.0 (TOE Server) and CYSECA Endpoint Application Control Client v1.1.12 (TOE Client). The TOE is an endpoint application control allows organization to enhance the defences against executing unwanted or malicious application on critical endpoint computer. TOE comprise of server and client components that can be operated in one or more instance.

The scope of the evaluation is defined by the Security Target (Ref [6]) which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2). This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by Securelytics SEF and the evaluation was completed on 24 September 2020.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at http://www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at http://www.commoncriteriaportal.org

It is the responsibility of the user to ensure that CYSECA Endpoint Application Control meets their requirements. It is recommended that a potential user of the TOE refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

CYSECA Endpoint Application Control consists of CYSECA Endpoint Application Control Server v1.2.0 (TOE Server) and CYSECA Endpoint Application Control Client v1.1.12 (TOE Client). The TOE is an endpoint application control allows organization to enhance the defences against executing unwanted or malicious application on critical endpoint computer. TOE comprise of server and client components that can be operated in one or more instance. Organisations are constantly facing threats that results in data leakage, locked folders with ransom note, loss of valuable data, use of compromised clients as launching pad for malicious activities and more.

The TOE includes the following security functions:

- Application Control (Whitelist)
- Audit
- Identification & Authentication
- Security Management
- Secure Communication

1.2 TOE Identification

The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C112
TOE Name	CYSECA ENDPOINT APPLICATION CONTROL
TOE Version	CYSECA Endpoint Application Control which consists of: • CYSECA Endpoint Application Control Server v1.2.0 • CYSECA Endpoint Application Control Client v1.1.12
Security Target Title	CYSECA Endpoint Application Control Security Target
Security Target Version	V1.0
Security Target Date	20 September 2020
Assurance Level	Evaluation Assurance Level 2

Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant
Sponsor	Pernec Integrated Network Systems Sdn Bhd
Developer	Pernec Integrated Network Systems Sdn Bhd
Evaluation Facility	Securelytics SEF

1.3 Security Policy

There is no organisational security policies defined regarding the use of TOE.

1.4 TOE Architecture

The TOE includes both physical and logical boundaries which are described in Section 1.5 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

The TOE consists of the following security functions identified in the Security Target (Ref [6]).

Table 2: CYSECA Endpoint Application Control Logical Boundaries

Application Control (Whitelist)	The TOE is designed to prevent executing unauthorized application, unknown application, malware and zero-day malware on client. The TOE can be configured to allow authorised application to execute on client to prevent execution of unauthorized application, unknown application, malware and zero-day malware.
Audit	The TOE generates audit records for security events. Super Admin, Admin and Read-Only users have the ability to view and export the audit and transaction logs. The TOE

	generates audits when events, file-less and action occur, stores the audit information on the client local system, transmits the audit information to a server, generates alarms for designated events, and provides a means for audit review. Protection of audit data in the audit trail involves the TOE and the operating System (OS). The TOE controls the insertion of audit events into the audit log and the deletion of audit events from the audit log. The OS provides basic file protection services for the audit log.
Identification and Authentication	TOE users (Super Admin, Admin and Read-Only) are required to identify or authenticate with the TOE prior to any user action or information flow being permitted. TOE users may interact with the TOE via supported web browsers.
Security Management	The TOE provides Super Admin and Admin with the capabilities to configure, monitor and manage the TOE to fulfil the Security Objectives. The TOE restricts access to the management functions based on the role of the user. Security management principles relate to Application Control Rules and Audit.
Secure Communications	The TOE utilized Transport Layer Security (TLS) v1.2 cryptographic protocol to secure the communication between client web browser and the TOE.

1.4.2 Physical Boundaries

Product components included in the TOE are listed below. Figure 1 illustrates a representative diagram of the TOE in its evaluated configuration.

- CYSECA Endpoint Application Control Server
- CYSECA Endpoint Application Control Client
- User Interface

At a high level, the TOE process flow includes the following:

- Software process flow for connection to internal TOE components and external IT products.

- Software process flow to receive and process traffic from internal TOE components and external IT products.
- User interface process flow to handle administrative actions.

CYSECA Endpoint Application Control product components excluded from the TOE in the evaluated configuration are:

- Operating Systems
- Web Server components
- CYSECA Master Server

The following diagram is a representation of the evaluated configurations of the TOE and its components.

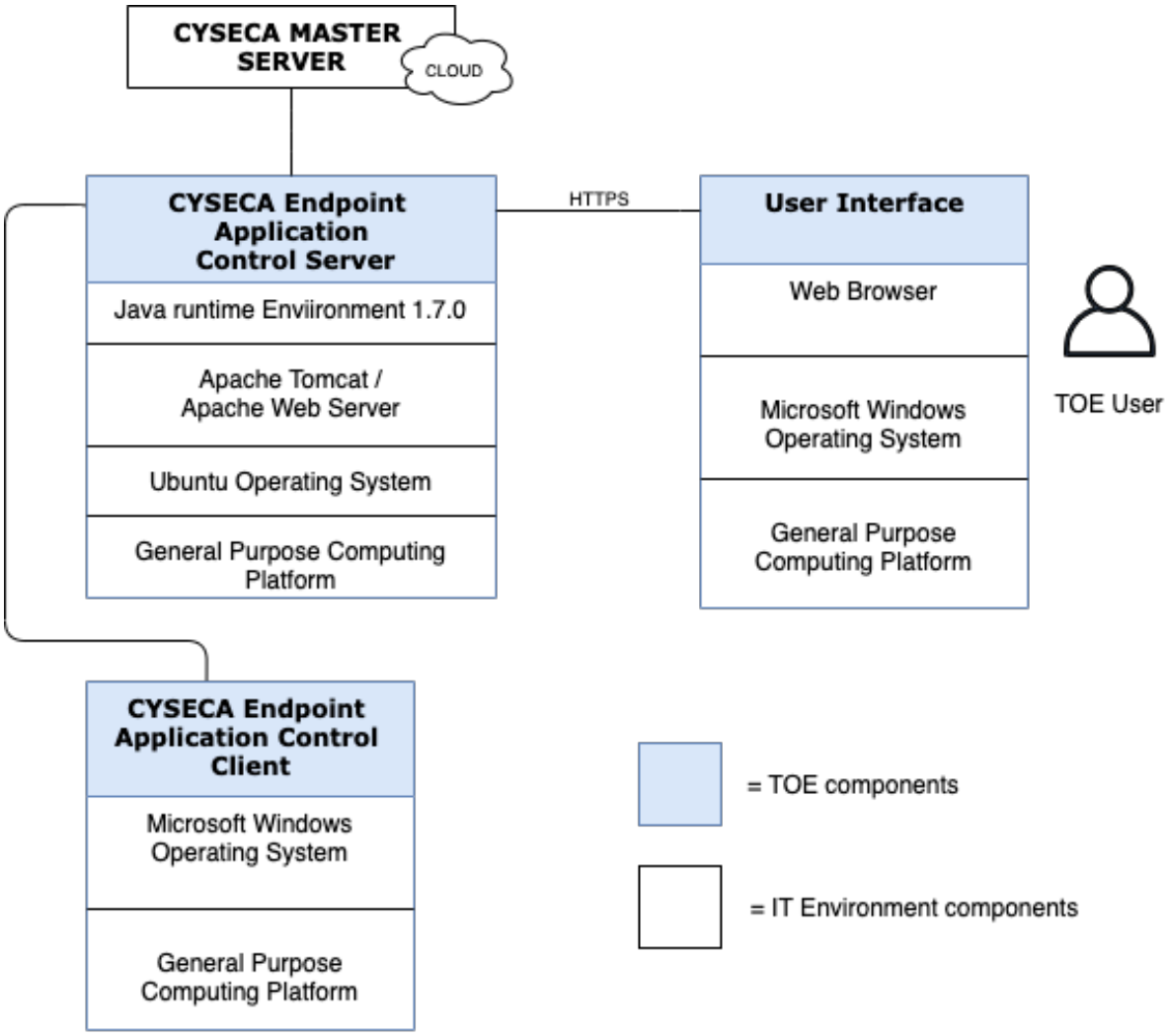

Figure 1: TOE Boundary

1.5 Clarification of Scope

The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]).

Potential consumers of the TOE are advised that some functions and services of the overall product have not been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

This section summarises the security aspects of the environment/configuration in which the product is intended to operate. Consumers should understand their own IT environment and requirements for secure operation of the TOE as defined in the Security Target (Ref [6]).

1.6.1 Operational Environment Assumptions

Assumptions for the TOE environment as described in the Security Target (Ref [6]):

Table 3: Assumptions for the TOE environment

Assumption	Statements
A.PLATFORM	It is assumed that the TOE relies upon a trustworthy platform and local network from which it provides administrative capabilities. The TOE relies on this platform to provide logon services via a local or network directory services, and to provide basic audit log management functions. The platform is expected to be configured specifically to provide TOE services, employing features such as a host-based firewall which limits its network role to providing TOE functionally.
A.ADMIN	It is assumed that one or more competent, trusted personnel who are not careless, wilfully negligent, or hostile, are assigned and authorized as the

Assumption	Statements
	Administrator, and do so using and abiding by guidance documentation.
A.USER	It is assumed that users are not wilfully negligent or hostile and use the device within compliance of a reasonable enterprise security policy.
A.TIMESTAMP	It is assumed that the platforms on which the TOE operate shall be able to provide reliable time stamps.
A.PHYSICAL	It is assumed that the appliance hosting the operating system and database are in a secure operating facility with restricted physical access and non-shared hardware.

1.7 Evaluated Configuration

The TOE's evaluated configuration requires one or more instances of a TOE Client, one instance of a TOE Server, and one or more instances of a workstation for management via User Interface.

PERNEC representative will install TOE server on-premise or cloud infrastructure. The pre-configured TOE Client Installer (Agent) will be distributed to endpoint client. The TOE Server's credential will be shared to the TOE Super Admin.

1.8 Delivery Procedures

The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

The delivery procedures should consider, if applicable, issues such as:

- ensuring that the TOE received by the consumer corresponds precisely to the evaluated version of the TOE;
- avoiding or detecting any tampering with the actual version of the TOE;
- preventing submission of a false version of the TOE;

- avoiding unwanted knowledge of distribution of the TOE to the consumer: there might be cases where potential attackers should not know when and how it is delivered;
- avoiding or detecting the TOE being intercepted during delivery; and
- avoiding the TOE being delayed or stopped during distribution.

1.8.1 TOE Delivery

1.8.1.1 Hardware delivery

The delivery of the TOE from the build environment to the development goes through the following phases:

a. Receiving Customer Order

Responsibilities: Sales

- Received with written/verbally Order from Customers through email/telephone conversation

b. Evaluate Customer's Order

Responsibilities: Sales Dept. Head

- To evaluate with customer the exact product requirements, quantity and pricing

c. Planning Stock Delivery

Responsibilities: Sales Dept. Head/Production Manager

- To determine the stock delivery schedule and executive

The TOE is wrapped in a plastic bag to provide resistance against moisture. Each TOE is then enclosed in cardboard shipping boxes and sealed with tape that contain Pernec logo. A shipping label identifying the exact product (including the serial number for the included device) and the customer name is provided on the outside of the box

d. Product Requisition

Responsibilities: Sales/Sales Coordinator

- To determine the stock delivery schedule and executive to raise Sales Requisition to Production/Stock Controller to inform Product delivery schedule to Production and Store Personnel

e. Product Delivery Arrangement

Responsibilities: Sales/Store Personnel

- Store Personnel to prepare product model and quantity required

f. Product Delivery

Responsibilities: Sales/Store Coordinator

- To execute the product delivery to customer based on the quantity required and schedule agreed

g. Invoicing

Responsibilities: Sales/Sales Coordinator/Store Personnel

- To ensure the product model quantity are correct and deliver according the agreed delivery schedule. Proceed to Invoice when product being delivered

1.8.1.2 Software Delivery

PERNEC representative will install TOE server on-premise or cloud infrastructure. The pre-configured TOE Client Installer (Agent) will be distributed to endpoint client. The TOE Server's credential will be shared to the TOE Super Admin.

2 Evaluation

The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2. The evaluation was performed conformant to the ISCB Product Certification Schemes Policy (Product_SP) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators confirmed that the TOE provided for evaluation is labelled with its reference and the TOE references used are consistent.

The evaluators examined that the method of identifying configuration items and determined that it describes how configuration items are uniquely identified

The evaluators examined the configuration items in the configuration item list and determined that they are identified in a way that is consistent with the CYSECA Endpoint Application Control Life Cycle Documentation version 1.0.

2.1.2 Development

Architecture

The evaluators examined the security architecture description (contained in [24]) and determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

The security architecture description describes the security domains maintained by the TSF.

The initialisation process described in the security architecture description preserves security.

The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

Functional Specification

The evaluators examined the functional specification and determined that:

- The TSF is fully represented;
- It states the purpose of each TSF Interface (TSFI); and
- The method of use for each TSFI is given.

The evaluators also examined the presentation of the TSFI and determined that:

- It completely identifies all parameters associated with every TSFI; and
- It completely and accurately describes all error messages resulting from an invocation of each SFR-enforcing TSFI.

The evaluators also confirmed that the developer supplied tracing links of the SFRs to the corresponding TSFIs.

TOE Design Specification

The evaluators examined the TOE design (contained in [24]) and determined that the structure of the entire TOE is described in terms of subsystems.

The evaluators also determined that all subsystems of the TSF are identified.

The evaluators determined that interactions between the subsystems of the TSF were described.

The evaluators examined the TOE and determined that each SFR supporting or SFR-non-interfering subsystem of the TSF was described such that the evaluators could determine that the subsystem is not SFR-enforcing.

The evaluators found the TOE design to be a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

The evaluators examined the TOE design and determined that it provides a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

The evaluators determined that the TOE design contained a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

The evaluators determined that all SFRs were covered by the TOE design, and concluded that the TOE design was an accurate instantiation of all SFRs.

2.1.3 Guidance documents

The evaluators examined the operational user guidance determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

The evaluators examined the operational user guidance in conjunction with other evaluation evidences and determined that the guidance identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

The evaluators determined that the operational user guidance describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

The evaluators confirmed that the TOE guidance fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

Testing at EAL 2 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by Securelytics SEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Report.

2.1.4.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator). The results of the evaluators' tests are consistent with the developers' test results defined in their evaluation evidences submitted.

2.1.4.2 Independent Functional Testing

At EAL 2, independent functional testing is the evaluation conducted by evaluators based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a subset of the developer's test plan, and creating test cases that are independent of the developer's tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

Table 4: Independent Functional Test

TEST ID	DESCRIPTIONS	RESULTS
F001 – Security Audit TSFI: Management Interface	1. To verify that TOE able to: a. Provide record within each audit records • Data and time of the events • Type of events • MD5 • Path • Command Line • Package • Subject identity (if applicable) • Outcome of the event b. Generate an audit report for every level of auditable events • Action logs – Date &time, Username, IP Address, Event Type • Event Logs – Date&time, MD5, Path, Computer and Package • Fileless Logs – Time, Command Line, Computer 2. To verify that Super Admin, admin and Read-only able to read all information from audit records	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
F002 – Security Management Data Protection TSFI: Management Interface	To verify that the TOE able to enforce control SFP and perform management function as below: Super Admin: • Dashboard Select/View authorised dashboard information • Manage >Branches Add/Delete/Change/View list of Administrator • Clients Select/Import/View client's Group • Rules Add/Delete Groups Duplicate Application Rules Allow/Disallow Application Rules • Samples Export List File Samples Expert List Certificate Samples View File Verdict View Certificate Verdicts • Logs Export/View Event Logs Export/View Fileless Logs Export/View Action Logs Generate Report	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	• Reports Clear/Select/View Branch Select Date Generate report • CYSECA **>Settings** Website/Proxy/SMTP Configuration Enable/disable Auto Whitelisting Configure Client's Agent Updates Configure Rules, Agent Database and Automatic Whitelisting View License Enable/Disable email to admins when license status changed Configure the Archive Database Update Syslog Configuration Configure Ping Interval **>Profile** View Profile Information Update Password Verify Email >About View Information View Terms and Conditions View Privacy Policy View Third-Part Notices	

TEST ID	DESCRIPTIONS	RESULTS
	>Logout	
F003 – Security Management Data Protection TSFI: Management Interface	To verify that the TOE able to enforce control SFP and perform management function as below: Admin: • Dashboard Select/View authorised dashboard information • Branches Add/Delete/Change/View list Branches Add/Delete/Change/View list of Administrator • Clients Add/Delete/Change/View authorised client's Group • Rules Add/Delete Groups Duplicate Application Rules Allow/Disallow Application Rules • Samples Export List File Samples Expert List Certificate • Logs Export/View Event Logs Export/View Fileless Logs	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	Export/View Action Logs • Reports Clear/Select/View Branch Select Date Generate report • CYSECA **>Settings** Website/Proxy/SMTP Configuration Enable/disable Auto Whitelisting Configure Client's Updates Configure Rules, Agent Database and Automatic Whitelisting View License Enable/Disable email to admins when license status changed Configure the Archive Database Update Syslog Configuration Configure Ping Interval **>Profile** View Profile Information Update Password Verify Email **>About** View Information View Terms and Conditions View Privacy Policy	

TEST ID	DESCRIPTIONS	RESULTS
	View Third-Part Notices **>Logout**	
F004 – Security Management Data Protection TSFI: Management Interface	To verify the TOE able to enforce the access control SFP and perform management function as below: Read only: • Dashboard Select/View All Branches Server dashboard information • Branches View list of Branches View client(s) • Rules View Allow/Disallow Application Rules • Samples Export List File Samples Export List Certificate Samples View File Verdicts View Certificate Verdicts • Logs Export/View Event Logs Export/ View Fileless Logs Export/View Action Logs • Report Clear/Select/View Branch	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	Select Date Generate Report • CYSECA >Settings Website/Proxy/SMTP Configuration Enable/Disable Auto Whitelisting Configure Client's Agent Updates Configure Rules, Agent Database and Automatic Whitelisting View License Enable/Disable email to admins wen license status changed Configure the Archive Database Update Syslog Configuration Configure Ping Interval >Profile View Information View Terms and Conditions View Privacy Policy View Third-Party Notices >Logout	
F005 – Data Protection TSFI: Management Interface	1. To verify that the TOE allow access if detect User Interface running on existing session, IP address and devices 2. To verify that the TSF deny access if detect user interface running on different session, IP address and devices and required termination code	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	to terminate previous session and continue with new session	
F006 – Identification and Authentication Security Management TSFI: Management Interface	1. To verify that the TOE able maintain username and password of user 2. To verify that each user is successfully authenticated and identified before allowing any actions on behalf of the user 3. To verify that the TOE enforces SFP allow default values for security attributes which used to enforce SFP 4. To verify that the TOE allows none to override default values when object or information is created	Passed. Result as expected.
F007 – Secure Communication TSFI: TLS_API	1. To verify that the TOE use SSL v2/v3 and TLS v1 to protect the communicated data from modification and disclosure. 2. To verify that the TOE allows remote users to initiate communication via trusted path	Passed. Result as expected.
F008 – Application Control	1. To verify that TSF able to collection inform from targeted client system resources as follow: a. A whitelist inventory of program code, including binary executable command line and scripts b. Events indicating prevented unauthorised executions of program code	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	2. To verify that System able to collect and record application name and object name for application control 3. To verify that System able to compare and application rules of any client application attempting to execute to an on the client with the whitelist to determine whether it has permission	

All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration testing

The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design, and security architecture description.

From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other requirement for exploitation

The evaluators' search for vulnerabilities also considered public domain sources for published vulnerability data related to the TOE and the contents of all TOE deliverables. The following public domain sources were searched:

a) www.google.com

b) www.yahoo.com

c) www.bing.com

d) https://cve.mitre.org

The penetration tests focused on:

a) SQL Injection;

b) Server-Side Template Injection;

c) Cross site scripting;

d) Failure to restrict URL Access;

e) Directory Traversal;

f) Rate Limit for Session Code;

g) Sensitive Data Exposure – Browser;

h) Weak Password;

i) Input Validation;

j) Error messages;

k) Sensitive Data Exposure – Server;

l) Windows Privilege Escalation – Unquoted Service Path;

m) Improper Folder Permission;

n) Bypass application restriction;

o) Sensitive Data Exposure – Windows Registry; and

p) User Account Lockout.

The result of the penetration testing noted that there is no residual vulnerability found. However, it is important to ensure that the TOE is used only in its evaluated configuration and in a secure environment as specified in Section 1 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. Therefore, the certifiers confirmed that all tests conducted were PASSED as expected.

3 Result of the Evaluation

After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of CYSECA ENDPOINT APPLICATION CONTROL performed by Securelytics SEF.

Securelytics SEF found that CYSECA ENDPOINT APPLICATION CONTROL upholds the claims made in the Security Target (Ref [6]) and supporting documentations and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2.

Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

EAL 2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and complete interface specifications, guidance documentation and a description of the design of the TOE to understand the security behaviours.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

3.2 Recommendation

The Malaysian Certification Body (MyCB) is strongly recommending that:

a) Potential purchasers of the TOE should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings

b) Potential purchasers of the TOE must maintain the confidentiality, integrity and availability of security relevant data for TOE initialization, start-up and operation if stored or handled outside the TOE.

c) System Auditor should review the audit trail generated and exported by the TOE periodically.

d) Potential purchasers of the TOE must ensure appropriate network protection is maintained, the network on which the TOE is installed must be both physically and logically protected.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July, 2014.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[3] The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] ISCB Product Certification Schemes Policy (Product_SP), v1b, CyberSecurity Malaysia, March 2018.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v1a, March 2018.

[6] Cyseca Endpoint Application Control Security Target, Version 1.0, 20 September 2020.

[7] Cyseca Endpoint Application Control, Evaluation Technical Report, Version 1.0, 8 Oct 2020.

[8] Cyseca Endpoint Application Control Design Documentation, Version 1.0, 20 September 2020

A.2 Terminology

A.2.1 Acronyms

Table 5: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility

Acronym	Expanded Term
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 6: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.

Term	Definition and Source
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---