MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

C147 Certification Report
Symantec™ Data Center Security: Server Advanced v6.10

File name: ISCB-3-RPT-C147-CR-v1
Version: v1
Date of document: 16 May 2026
Document classification : PUBLIC

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

C147 Certification Report

Symantec™ Data Center Security: Server Advanced v6.10

16 May 2026

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:	C147 Certification Report
DOCUMENT REFERENCE:	ISCB-3-RPT-C147-CR-v1
ISSUE:	v1
DATE:	16 May 2026
DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

The copyright of this document, which may contain proprietary information, is the property of CyberSecurity Malaysia.

The document shall be held in safe custody.

©CYBERSECURITY MALAYSIA, 2026

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 200601006881 (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.

The Certification Report, Certificate of the evaluated product, and the Security Target (Ref [6]) have been published on the MyCC Scheme Certified Product Register (MyCPR) at https://iscb.cybersecurity.my and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Reproduction of this report is authorised provided the report is reproduced in its entirety.

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 2022 revision 1 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 2022 revision 1 (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	4 May 2026	All	Initial draft
d2	11 May 2026	4, 7, 12, 13	Amendment from the comments of reviewers.
v1	16 May 2026	All	Final version of the document.

Executive Summary

The project is C147 Symantec™ Data Center Security: Server Advanced v6.10, referred to as the Target of Evaluation (TOE) which developed by Symantec Corporation. The primary purpose of the TOE is to provide Intrusion Prevention and Detection services to monitor, control, detect, and respond to endpoint and network threats. The TOE provides this service by monitoring and protecting physical and virtual network endpoints and data centers using a combination of host-based intrusion detection, intrusion prevention, least privilege access control.

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 Augmented with ALC_FLR.1 (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 Security Evaluation Facility (SEF) and the evaluation was completed on 17 April 2026.

This Certification Report is associated with the Certificate of Product Evaluation dated 21 May 2026 and the Security Target (Ref [6]). The certification is valid for a period of five (5) years from the date of the Certificate of Product Evaluation, after which it will expire.

It is the responsibility of the user to ensure that Symantec™ Data Center Security: Server Advanced v6.10 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

1 The Symantec™ Data Center Security: Server Advanced v6.10 is a Host-Based Intrusion Prevention System and a Server Security Management solution. The TOE is a software that provides a comprehensive, policy-based security layer for heterogeneous server and endpoint to prevent zero-day exploits and ensure continuous compliance, offering more granular controls than typical desktop endpoint security solutions.

2 The TOE consists of the following components:

- Management Server – the Management Server provides the following capabilities:
  - Secure communications with other TOE components
  - Policy storage and coordination of policy distribution
  - Management of agent event logging and reporting
  - Bulk event file storage management for efficient archival storage of all logged events
  - Alert processing (SMTP, SNMP, file), data purging, and other management functions
  - REST API – a fully instrumented REST API that provides a corresponding API for all actions, enabling full internal and external cloud automation.
- Communication Server – The Communication Server provides the following capabilities:
  - Secure communication with Agents and the Management Server
  - Agent Registration and coordination of policy distribution to the Agents
  - Policy and Event processing.

  Agents report events to the Communication Server for storage and are viewed in the Management Console. TLS versions 1.2 and 1.3 secures communication between Communication Server and the Agents.
- Agents – software components that enforce policy on the endpoint computers on which they are installed. Each agent enforces rules that are expressed in policies, thereby controlling and monitoring application and user behavior on the endpoint. Agents provide the following capabilities:

  - Download of policies and settings from the Communication Server and upload of events and status information to the Communication Server
  - Interception if system calls to enforce prevention policies
  - Monitoring of system change events and log files in accordance with detection policies
  - Agent configuration and diagnostic support
  - Native support for Windows, UNIX and Linux servers and workstations
  - Support on VMWare guest systems for detection and prevention with any of the operating systems that are natively supported
  - Remote monitoring of hosts without a native agent (only detection features are available in this mode).

- Management Console – interface for performing administrative tasks including policy management, configuration management and user management.
- Database – the database store policies, agent information, and real-time actionable events. It is accessible through JDBC/ODBC. The System Administrator can configure encrypted communications between the database and the Management Server and Communication Server.

3 The Management Server, Communication Server, and Management Console run on Windows operating systems. The agents run on Windows, UNIX and Linux operating systems. Agents report events to the Communication Server for storage and are viewed in the Management Console. Agent log rules control the events that are logged for that agent. Logged data includes event date and time, event type, importance rating, and any prevention action performed. Dashboards in the Management Console provide charts and graphs displaying aggregated summary data about events, agents, and policies. The TOE uses Transport Layer Security (TLS) using X.509 certificates with SHA-256 to secure communications between its various components.

4 The TOE provides the following features:

- Security Audit – The TOE generates and securely storage audit records of security-relevant events
- Identification & Authentication – The TOE manages authorized user accounts

- Security Management – Those responsible for administering the TOE use the management console to control security functions with role-based access restrictions
- Protection of the TSF – The TOE uses HTTPS to protect TSF data communicated between distributed components of the TOE
- TOE Access – The TOE ends inactive interactive sessions after a configurable period
- Trusted Path/Channels – HTTP-based trusted paths and channels for authentication and management.
- Intrusion prevention and detection – The TOE provides a policy-based approach to intrusion prevention and intrusion detection.

1.2 TOE Identification

5 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	C147
TOE Name	Symantec™ Data Center Security: Server Advanced
TOE Version	v6.10
Security Target Title	Symantec™ Data Center Security: Server Advanced v6.10 Security Target
Security Target Version	0.8
Security Target Date	8 May 2026
Assurance Level	Evaluation Assurance Level 2 Augmented with ALC_FLR.1
Criteria	Common Criteria for Information Technology Security Evaluation, November 2022, Version 2022, Revision 1 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, November 2022, Version 2022, Revision 1 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant

Sponsor	Leidos Inc. 6841 Benjamin Franklin Dr, Columbia, MD 21046, United States
Developer	Symantec Corporation 1320 Ridder Park Drive, San Jose, CA 95131, United States
Evaluation Facility	Securelytics SEF A-17-01, Tower A Atria Sofo Suites, Jalan SS 22/23, Damansara Utama, 47400 Petaling Jaya, Selangor, Malaysia

1.3 Security Policy

6 Agents use the following types of policies:

- **Preventions policies** – these confine on each process on a computer to its normal behavior. Programs that are identified as critical to system operation are given specific behavior controls, while generic behavior controls provide compatibility for other services and applications.
- **Detection policies** – these monitor events and syslogs, and report anomalous behavior. Features include policy-based auditing and monitoring; log consolidation for easy search, archival, and retrieval; event analysis and response capabilities; and file and registry protection and monitoring.

7 Agent policies have options that allow the System Administrator or Manager to configure a policy for assignment to a target computer. Policy options comprise a simplified set of controls that the System Administrator or Manager can use to enable or disable features in a policy. Some options have parameters, which provides even further customization

1.4 TOE Architecture

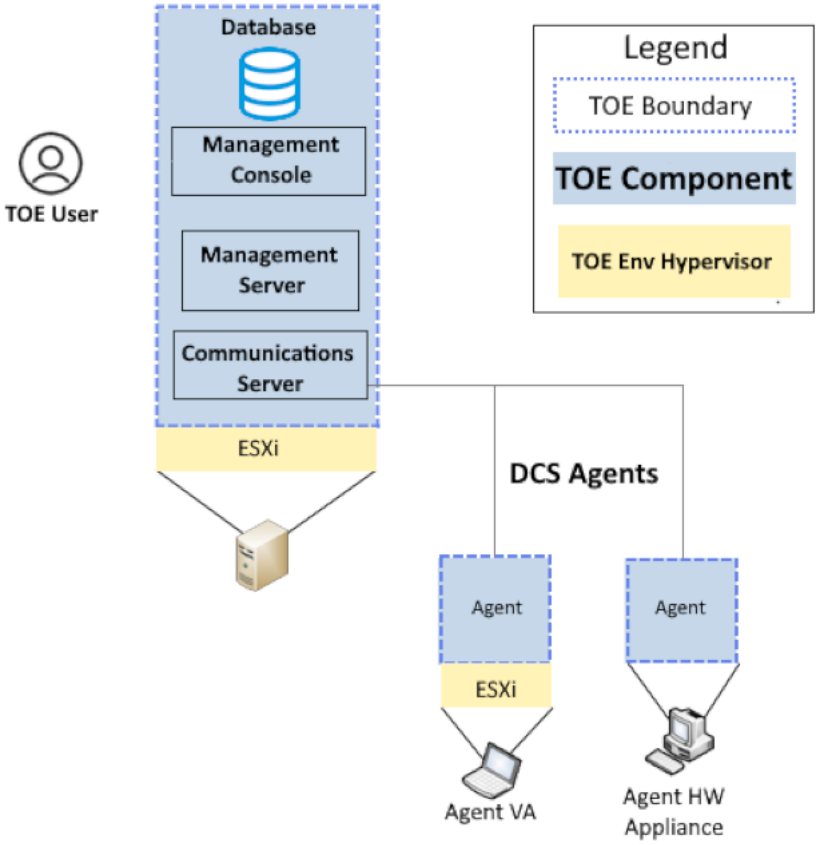

Figure 1: TOE Architecture

8 The TOE includes only logical boundaries which are described in Section 2.2 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

9 The TOE consists of security functions provided by the TOE that are identified in the Security Target ([6]).

Table 2: TOE Logical Boundaries

Security Audit	The TOE is able to generate audit records of security-relevant events, which it stores in the Management Server database. The database protects the stored audit records from unauthorized modification and deletion. The TOE provides System Administrators with capabilities to review the generated audit records, including capabilities to review

	the generated audit records, including capabilities for searching audit records based on the values in specified audit records fields and to filter records based on audit event type and period of time.
Identification and Authentication	The TOE maintains accounts of the authorized users of the system. The user account includes the following attributes associated with the user: username; password; roles; and e-mail address information. This information is stored in the Management Server database. The TOE supports user authentication with local-defined passwords and remote authentication using Active Directory. The TOE enforces password complexity requirements that dictate that the password is at least eight characters in length, contains at least one upper case character, contains at least one lower case character, contains at least 1 number, and contains at least 1 special character (! @ # $ % ^ & - + = ( ) { } _]). The TOE enforces an account lockout mechanism triggered by failed authentication attempts.
Security Management	TOE users with the System Administrators or Managers role manage the TOE and its security functions using the Management Console, which provides access to all of the TOE's security management functions. The TOE provides the following default security management roles for the Management Console: System Administrators; Managers; and Viewers (which does not provide any security management capability). The TOE enforces restrictions on which management capabilities are available to each role.
Protection of the TSF	The TOE uses HTTPS to protect TSF data communicated between distributed components of the TOE.
TOE Access	The TOE will terminate interactive sessions after a period of inactivity configurable by a System Administrator. By default, interactive sessions are terminated after 30 minutes of inactivity. The TOE also allows user-initiated termination of the user's own interactive session by explicitly logging off.

Trusted Path/Channels	The TOE provides a trusted path for TOE System Administrator or Managers to communicate with the TOE via its REST API. Users of the TOE with a any role initiate the trusted path by establishing an HTTPS connection. The trusted path is used for initial authentication and all subsequent administrative actions. The use of HTTPS ensures all communication over the trusted path is protected from disclosure and modification.
Intrusion Prevention and Detection	The TOE provides a policy-based approach to intrusion prevention and intrusion detection. The TOE is able to control and monitor what programs and users can do to computers. Agent software at the endpoints controls and monitors behavior based on policy. The TOE policy library contains prevention and detection policies that a System Administrator or Manager can deploy and customize to protect the network and endpoints. Agents enforce rules specified in prevention policies to control how processes running on the protected asset access resources, such as other processes, memory, files, registry keys (on Windows-based assets) and network connections. Agents apply rules configured in detection policies to collect IDS data from monitored resources such as Windows event logs, text logs, registry keys, files, syslog daemons and UNIX wtmp files. In response to identified violations of prevention and detection policies, agents can generate events that are stored in the Management Server database. The database protects the stored events from unauthorized modification and deletion. The TOE can monitor the events stored in the database against configured filter rules and generate alerts if a configured minimum number of events occur in a configured time window. When an alert is generated, a notification can be sent to configured alert destinations, including email addresses, an SNMP server or a text file. The TOE also provides capabilities for TOE System Administrators, Managers, and Viewers to review generated

	events, including capabilities for searching events based on the values in specified event fields and to filter events based on event type and period of time.

1.4.2 Physical Boundaries

10 This is a software only TOE. No hardware is included in the TOE Boundary.

1.5 Clarification of Scope

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

12 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]).

13 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

14 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

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

Table 3: Assumptions for the TOE environment

Assumption	Statements
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.PLATFORM	The underlying operating system of each TOE component will protect the component and its configuration from unauthorized access.

Assumption	Statements
A.PROTECT	The hardware hosting the TOE software and the TOE software critical to security policy enforcement will be located within controlled access facilities which will prevent unauthorized physical access.

1.7 Evaluated Configuration

16 The evaluated configuration of the TOE will have all Server components (Management Console, Management Server, Communication Server) installed on a single Windows 2019 server machine, and the TOE agent residing on a Windows 11 endpoint. The specifications of the 2 machines are as follows:

Table 4: Evaluated Configuration

Assumption	Operating System (non-TOE)	Hardware Machines Specifications (non-TOE)
Server **Management Console** **Management Server** **Communication Server**	Windows Server 2019 Advanced Edition	64-bit (x86_64), four-core CPU, 16GB RAM, 150GB hard drive storage
Agent	Windows 10 Enterprise	64-bit (x86_64), two-core CPU, 4GB RAM, 50GB hard drive storage

17 Within the Management Console, there are three (3) roles that can be selected from when creating or editing a user. Additional custom roles can be created; however, in the CC Evaluated Configuration, only the 3 default roles were used. Following are the 3 default roles used:

- System Administrator
- Manager
- Viewer

18 These roles determine whether changes can be made to the TOE's configuration and control whether some functionality is even visible to a user role.

19 At a high level, the System Administrator has full read and write access to all configuration within the TOE. The Manager role has almost full read and write access to everything except for the following areas:

- Settings: User Management, Server Registry
- Integrations: Active Directory

20 The Viewer accounts can view all configurations and policies, but explicitly does NOT have access to the following areas:

- Settings: User Management, Certificates Server Registry, License
- Integrations: Active Directory

21 Refer to the Common Criteria Guidance Supplement ([6]) for further details. This document outlines the administrator functions and interfaces required to properly configure and maintain the TOE in its evaluated configuration.

1.8 Delivery Procedures

22 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.

23 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 Software Delivery

24 TOE software is provided to licensed customers via the Broadcom Support Portal that can be accessed at the following location: https://support.broadcom.com/group/ecx/downloads. The Broadcom Support Portal is only accessible over TLS 1.2 or TLS 1.3.

- To gain access to the Broadcom Support Portal, customers must first register an account at the Broadcom Support Portal and purchase the TOE.
- Once registered with Broadcom Support Portal, their entitlement is used to determine download permissions based on the purchase agreement. Customers can then navigate to the Broadcom Support Portal and download the TOE as per their entitlements.
- The TOE consists of two (2) files for download:
  - The server-side components (Management Server, Communications Server, and Management Console)
  - The Windows Agent
- Integrity of the download is verified utilizing a provided SHA-256 hash. Customers should compute the hash of the downloaded TOE software to ensure the values match.
- TOE software updates are provided to customers via the Broadcom Support Portal.
- The documentation is provided to the users via the Broadcom Tech Docs publishing site: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/data-center-security-(dcs)/6-10-1.html

25 To receive notifications when new TOE software is available (in addition to the TOE software advisories, security advisories, and critical alerts), Customers should click on their username in the top right, followed by “Notification Settings” within the Support Portal, search for “Data Center Security” and ensure all notifications are toggled on.

1.9 Flaw Reporting Procedures

26 The evaluator examined the flaw remediation procedures documentation and determined that it describes the procedures used to track all reported security flaws in each release of the TOE.

27 The evaluator examined the flaw remediation procedures documentation and determined that the application of these procedures would produce a description of each security flaw in terms of its nature and effects.

28 The evaluator examined the flaw remediation procedures and determined that the application of these procedures would identify the status of finding a correction to each security flaw.

29 The evaluator checked the flaw remediation procedures and determined that the application of the procedures would identify the corrective action for each security flaw.

30 The evaluator examined the flaw remediation procedures documentation and determined that it describes a means of providing the TOE users with the necessary information on each security flaw.

31 Therefore, the evaluator confirms that the information provided meets all requirements for content and presentation of evidence.

2 Evaluation

32 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 2022 Revision 1 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 2022 Revision 1 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 Augmented with ALC_FLR.1. The evaluation was performed conformant to the MyCC Scheme Requirement (MyCC_REQ) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

34 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

35 The evaluators confirmed that the configuration list includes TOE itself, the parts that comprise the TOE the evaluation evidence required by the SARs in the Security Target (Ref [6]).

36 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

2.1.2 Development

Architecture

37 The evaluators examined the security architecture description (contained in Section 4) 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.

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

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

40 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

41 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.

42 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.

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

TOE Design Specification

44 The evaluators examined the TOE design (contained in [8]) and determined that the structure of the entire TOE is described in terms of subsystems.

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

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

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

48 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.

49 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.

50 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

51 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.

52 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.

53 The evaluators examined the operational user guidance in conjunction with other evaluation evidence 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.

54 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.

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

56 The documents for TOE users to refer as guidance are as per listed:

- Symantec™ Data Center Security: Server Advanced v6.10 Common Criteria Guidance Supplement Evaluation Assurance Level (EAL): EAL2+ Document Version:0.2, 19 February 2026.

2.1.4 IT Product Testing

57 Testing at EAL 2 Augmented with ALC_FLR.1 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

58 The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, as documented in the Evaluation Technical Report (Ref [8]) (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 evidence submitted.

2.1.4.2 Independent Functional Testing

59 At EAL 2 Augmented with ALC_FLR.1, 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.

60 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 5: Independent Functional Test

TEST ID	DESCRIPTIONS	RESULTS
F001 – Security Audit FAU_GEN.1.1, FAU_GEN.1.2, FAU_SAR.1.1, FAU_SAR.1.2, FAU_SAR.2.1	1. To verify that the TOE able to generate audit data of the following auditable events: a. Start-up and shutdown of the audit functions; b. All auditable events for the [not specified] level of audit; and	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	c. The following auditable events: i. Reading of information from the audit records ii. All use of the authentication mechanism iii. All use of the user identification mechanism iv. All modifications in the behavior of the functions of the TSF v. All modifications to the values of TSF data vi. Use of the management functions vii. Modifications to the group of users that are part of a role 2. To verify that the record within the audit data at least the following information: a. Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; b. For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, [none]. 3. To verify that the TOE provide [System Administrators, Managers	

TEST ID	DESCRIPTIONS	RESULTS
	and Viewers] with the capability to read [all audit information] from the audit data. 4. To verify that the TOE provide the audit data in a manner suitable for the user to interpret the information. 5. To verify that the TOE prohibit all users read access to the audit data, except those users that have been granted explicit read-access.	
F002 – Security Audit FAU_SAR.3.1	To verify that the TOE provide the ability to apply searches and filtering] of audit data based on the following criteria: a. Searches based on values of specified audit record fields and combinations of logical and conditional operators b. Filtering based on audit event type and period of time.	Passed. Result as expected.
F003 – Security Audit FAU_STG.2.1, FAU_STG.2.2	1. To verify that the TOE protect the stored audit in the audit trail from unauthorized deletion. 2. To verify that the TOE is able to [prevent] unauthorized modification to the stored audit data in the audit trail.	Passed. Result as expected.
F004 – Identification and Authentication FIA_AFL.1.1, FIA_AFL.1.2	1. To verify that the TOE detect when [System Administrator configurable positive integer within [two-ten]] unsuccessful authentication attempts occur related to [user logon].	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	2. To verify when the defined number of unsuccessful authentication attempts has been [met], the TSF shall [lock the user out until the lockout duration passes or the account is reset by a System Administrator].	
F005 – Identification and Authentication FIA_ATD.1.1	To verify that the TOE maintain the following list of security at tributes belonging to individual users: a. User Identity b. Password c. Roles d. E-mail address	Passed. Result as expected.
F006 – Identification and Authentication FIA_SOS.1.1	To verify that the TOE provide a mechanism to verify that secrets meet [the following constraints for all user accounts: a. Minimum length of eight characters b. Maximum length of twenty characters c. At least one upper case d. At least one lower case e. At least one number f. At least one of the following: ! @ # $ % ^ & - + = ( ) { } _	Passed. Result as expected.
F007 – Identification and Authentication FIA_UAU.2.1, FIA_UID.2.1	1. To verify that the TOE require each user to be successfully authenticated before allowing any other TSF-	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	mediated actions on behalf of that user. 2. To verify that the TOE require each user to be successfully identified before allowing any TSF- mediated actions on behalf of that user.	
F008 – Identification and Authentication FIA_UAU.5.1, FIA_UAU.5.2	1. To test that the TOE provide local passwords, support for remote authentication using Active Directory to support user authentication. 2. To test that the TOE authenticate any user's claimed identity according to the authentication method configured for the user account, either: a. local password-based authentication of user identities, or b. remote authentication using Active Directory username and password	Passed. Result as expected.
F009 – Security Management FMT_MOF.1.1	To verify that the TOE restrict the ability to modify the behavior of the functions security audit to System Administrators and Managers	Passed. Result as expected.
F010 – Security Management FMT_MTD.1.1(1), FMT_MTD.1.1(2), FMT_MTD.1.1(3), FMT_MTD.1.1(4), FMT_MTD.1.1(5),	1. To test that the TOE restrict the ability to [modify, delete] the [assets] to [System Administrators and Managers]. 2. To test that the TOE restrict the ability to [modify, delete, [create]] the [security groups, alerts and	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
FMT_MTD.1.1(6), FMT_MTD.1.1(7), FMT_MTD.1.1(8), FMT_SMF.1.1	notifications] to [System Administrators and Managers]. 3. To test that the TOE restrict the ability to [[create]] the [policies] to [System Administrators, Managers]. 4. To test that the TOE restrict the ability to [modify, delete] the [policies] to [System Administrators, Managers]. 5. To test that the TOE restrict the ability to [modify, delete, [create]] the [configurations] to [System Administrators, Managers]. 6. To test that the TOE restrict the ability to [modify, delete, [create]] the [Management Console user accounts] to [System Administrators]. 7. To test that the TOE restrict the ability to [modify] the [System user accounts] to [System Administrators]. 8. To test that the TOE restrict the ability to [modify] the [password of another user] to [System Administrators]. 9. To test that the TOE is capable of performing the following security management functions: a. Manage assets b. Manage security groups c. Manage policies d. Manage configurations e. Manage Management Console user accounts and roles	

TEST ID	DESCRIPTIONS	RESULTS
	f. Manage alerts and notifications g. Manage user accounts h. Modify user passwords	
F011 – Security Management FMT_SMR.1.1, FMR_SMR.1.2	1. To test that the TOE maintain the roles: a. System Administrators b. Managers c. Viewers 2. To test that the TOE is able to associate users with roles.	Passed. Result as expected.
F012 – Protection of the TSF FPT_ITT.1	To test that the TOE protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.	Passed. Result as expected.
F013 – TOE Access FTA_SSL.3.1, FTA_SSL.4.1	1. To test that the TOE terminate a Management Console an interactive session after a [time period of 60 minutes has elapsed]. 2. To test that the TOE allow user-initiated termination of the user's own interactive session.	Passed. Result as expected.
F014 – Trusted Path/Channels FTP_ITC.1.1, FTP_ITC.1.2, FTP_ITC.1.3	1. To test that the TOE provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	2. To test that the TOE permit [another trusted IT product] to initiate communication via the trusted channel. 3. To test that the TOE initiate communication via the trusted channel for [remote authentication to a LDAP server].	
F015 – Trusted Path/Channels FTP_TRP.1.1, FTP_TRP.1.2, FTP_TRP.1.3	1. To test that the TOE provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [disclosure, [undetected modification]]. 2. To test that the TOE permit [remote users] to initiate communication via the trusted path. 3. To test that the TOE require the use of the trusted path for [initial user authentication, [all remote administrative actions]].	Passed. Result as expected.
F016 – Intrusion Prevention and Detection System IPB_IDC.1.1, IPD_RCT.1.1, IPD_RCT.1.2	1. To test that the TOE is able to collect IDS data from the following monitored resources, based on configured detection rules: [Windows event logs, text logs, registry keys, files, syslog daemon, C2 audit log, WTMP file, [TOE agent error messages, TOE agent status messages]].	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	2. To test that the TOE is able to generate an event in response to identified violations of [prevention, detection] policies. 3. To test that the TOE record within each event at least the following information: source of the event; date and time the event occurred; type of event; severity of event; description of event.	
F017 – Intrusion Prevention and Detection System IPD_PBP.1.1, IPD_PBP.1.2, IPD_PBP.1.3, IPD_PBP.1.4, IPD_RCT.1.1, IPD_RCT.1.2	1. To test that the TOE enforce an intrusion prevention policy to assets based on the following: a. Subjects: processes—name, user, group, command line arguments, signature flag, publisher name, file hash b. Resources: i. processes—name, user, group, command line arguments, signature flag, publisher name, file hash, permissions ii. memory—address, access permissions iii. files—name, access permissions iv. registry keys—name, access permissions v. network connections—IP address, TCP port, UDP port 2. To test that the TOE enforce the following rules to determine if an	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	operation among controlled subjects and controlled resources is allowed: [a process can perform a requested operation on a resource if the requested operation is not explicitly blocked by a policy rule]. 3. To test that the TOE explicitly authorize access of subjects to resources based on the following additional rules: [If the policy is set to "Disable Prevention", then all processes are allowed to access all resources]. 4. To test that the TOE explicitly deny access of subjects to resources based on the following additional rules: [If the policy is set to "Application Control", then all processes that are not part of the Windows operating system are prohibited from executing unless they are explicitly listed in the policy configuration]. 5. To test that the TOE is able to generate an event in response to identified violations of [prevention, detection] policies. 6. To test that the TOE record within each event at least the following information: source of the event; date and time of the event occurred; type of event; severity of event; description of event.	

TEST ID	DESCRIPTIONS	RESULTS
F018 – Intrusion Prevention and Detection System IPD_IER.1.1, IPD_IER.1.2, IPD_IER.1.3, IPD_IER.2.1	1. To test that the TOE provide [authorized users with the System Administrator] with the capability to read [all event data] from the generated events. 2. To test that the TOE provide the event data in a manner suitable for the user to interpret the information. 3. To test that the TOE prohibit all users read access to the event data, except those users that have been granted explicit read access. 4. To test that the TOE provide the ability to apply [searches and filtering] of event data based on [the following criteria: a. Searches based on values of specified event fields and combinations of logical and conditional operators b. Filtering based on event type and period of time	Passed. Result as expected.
F019 – Intrusion Prevention and Detection System IPD_RCT.2.1, IPD_RCT.2.2	1. To test that the TOE is able to trigger an alert: a. An event matches a configured filter rule, and b. A configured minimum number of events that should trigger an alert notification occur within a configured time window 2. To test that the TOE send a notification to configured	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	notification destinations, which can be: a. E-mail address b. SNMP server c. text file	
F020 – Intrusion Prevention and Detection System IPD_STG.1.1, IPD_STG.1.2	1. To test that the TOE protect the stored event data from unauthorized deletion. 2. To test that the TOE is able to [prevent] unauthorized modifications to stored event data.	Passed. Result as expected.

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

2.1.4.3 Penetration testing

62 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.

63 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

64 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) NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf)

d) OSSTMM 3 – The Open Source Security Testing Methodology Manual (https://www.isecom.org/OSSTMM.3.pdf)

e) OWASP Desktop App Security Top 10 (https://owasp.org/www-project-desktop-appsecurity-top-10/)

f) OWASP Top 10 API Security Risks – 2023 (https://owasp.org/APISecurity/editions/2023/en/0x11-t10/)

g) NIST National Vulnerability Database (NVD) (https://nvd.nist.gov/search)

65 The penetration tests focused on:

a) Injections;

b) Broken Authentication and Session Management;

c) Sensitive Data Exposure;

d) Improper Authorisation;

e) Insecure Communication;

f) Using Components with Known Vulnerabilities;

g) Insufficient Logging & Monitoring;

h) Broken Object Level Authorisation;

i) Broken Authentication;

j) Unrestricted Resource Compensation;

k) Broken Function Level Authorisation;

l) Unrestricted Access to Sensitive Business Flows;

m) Server-Side Request Forgery;

n) Security Misconfiguration; and

o) Improper Inventory Management.

66 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 4 of the Security Target (Ref [6].

2.1.4.4 Testing Results

67 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

68 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [8], the Malaysian Common Criteria Certification Body certifies the evaluation of Symantec™ Data Center Security: Server Advanced v6.10 performed by Securelytics SEF.

69 Securelytics SEF found that Symantec™ Data Center Security: Server Advanced v6.10 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 Augmented with ALC_FLR.1.

70 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

71 EAL 2 Augmented with ALC_FLR.1 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.

72 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.

73 EAL 2 Augment with ALC_FLR.1 also provides assurance through use of a configuration management system, the secure delivery procedures, and evidence of flaw remediation procedures.

3.2 Recommendation

74 The Malaysian Certification Body (MyCB) strongly recommends that:

a) The users should make themselves familiar with the develop guidance provided with the TOE and pay attention to all security warnings.

b) The users 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) The users must ensure appropriate network protection is maintained, the network on which the TOE is installed must be both physically and logically protected.

(*Disclaimer: Opinion and interpretations expressed herein are outside the scope of accreditation*)

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 2022, Revision 1, November 2022.

[3] The Common Methodology for Information Technology Security Evaluation, Version 2022, Revision 1, November 2022.

[4] MyCC Scheme Requirement (MYCC_REQ), v2, CyberSecurity Malaysia, April 2025.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v4, April 2025.

[6] Symantec™ Data Center Security: Server Advanced v6.10 Security Target, Version 0.8, 8 May 2026.

[7] Symantec™ Data Center Security: Server Advanced v6.10 Common Criteria Guidance Supplement Evaluation Assurance Level (EAL): EAL2+, Version 0.2, 19 February 2026

[8] Symantec™ Data Center Security: Server Advanced v6.10, Evaluation Technical Report, Version 1.2, 16 May 2026.

A.2 Terminology

A.2.1 Acronyms

Table 6: 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

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

A.2.2 Glossary of Terms

Table 7: 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 17065
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 ---