MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

C102 Certification Report

Forcepoint On-Premise Security 8.5

File name: ISCB-3-RPT-C102-CR-v1
Version: v1
Date of document: 25 June 2019
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

C102 Certification Report

Forcepoint On-Premise Security 8.5

25 June 2019

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:	C102 Certification Report
DOCUMENT REFERENCE:	ISCB-3-RPT-C102-CR-v1
ISSUE:	v1
DATE:	25 June 2019

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. 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 27 June 2019, 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	14 June 2019	All	Initial draft
v1	25 June 2019	All	Final version

Executive Summary

The Target of Evaluation (TOE) is the Forcepoint On-Premise Security 8.5 running on Forcepoint V-Series Security Appliances. The TOE is a unified solution providing data protection. On-Premise Security 8.5 provides an email gateway and web scanning services, as well as data loss prevention capabilities.

The TOE provides a data theft prevention solution to secure an organisation's data on and off the organisation network.

The protection provided by On-Premise Security is delivered by three main components, namely Forcepoint Web Security, Forcepoint DLP, and Forcepoint Email Security, and the supporting component Forcepoint DLP Endpoint.

These components work together to prevent security breaches, productivity loss, and legal issues that might arise due to inappropriate or careless browsing, email messaging and network usage habits. The components are managed using the Forcepoint Security Manager (FSM) and Forcepoint Security Appliance Manager (FSAM).

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) Augmented (ALR_FLR.2). 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 BAE System Lab - MySEF and the evaluation was completed on 4 June 2019.

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 Forcepoint On-Premise Security 8.5 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 TOE is a unified solution providing data protection. On-Premise Security 8.5 provides an email gateway and web scanning services, as well as data loss prevention capabilities.

2 The TOE provides data theft prevention solution to secure an organisation's data on and off the organisation network.

3 The protection provided by On-Premise Security is delivered by three main components, namely Forcepoint Web Security, Forcepoint DLP and Forcepoint Email Security, and the supporting component Forcepoint DLP Endpoint.

4 These components work together to prevent security breaches, productivity loss, and legal issues that might arise due to inappropriate or careless browsing, email messaging and network usage habits. The components are managed using the Forcepoint Security Manager (FSM) and Forcepoint Security Appliance Manager (FSAM).

5 The On-Premise Security solution is highly scalable according to customer strategy to address data theft and data loss. The Forcepoint Web Security, Forcepoint DLP and Forcepoint Email Security can be deployed individually to address specific customer needs for data theft and loss through specific organisation network activities.

6 These solutions can be physical on-premise installations, hybrid deployments or cloud-based deployments. The evaluated deployment of On-Premise Security consists of Forcepoint Web Security and Forcepoint Email Security components installed on Forcepoint V-Series Security Appliances with the other On-Premise Security components installed on customer-supplied on-premise platforms. The testing covered the deployment of the TOE on the physical V-series appliances and virtual appliances.

7 The major security features of the TOE include:

a) Security Audit

b) Cryptographic Support

c) User Data Protection

d) Identification and Authentication

e) Security Management

f) Protection of the TSF

g) Resources Utilization

h) TOE Access

1.2 TOE Identification

8 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	C102
TOE Name	Forcepoint On-Premise Security
TOE Version	8.5
Security Target Title	Forcepoint On-Premise Security 8.5
Security Target Version	Version 1.0
Security Target Date	4 June 2019
Assurance Level	EAL2 Augmented (ALC_FLR.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 Package conformant to EAL2 Augmented ALC_FLR.2
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive, Columbia, Maryland 21046
Developer	Forcepoint 10900 Stonelake Blvd, 3rd Floor, Austin, TX 78759
Evaluation Facility	BAE Systems Lab - MySEF Level 28, Menara Binjai, 2 Jalan Binjai, 50450 Kuala Lumpur, Malaysia

1.3 Security Policy

9 No organisational security policies have been defined regarding the use of the TOE.

1.4 TOE Architecture

10 The TOE includes both physical and logical boundaries which are described in Section 2.2 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

11 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality:

a) Security Audit

The TOE generates audit logs of Forcepoint Security Manager activity; recording administrator login attempts, logoffs, policy changes, and configuration changes in the Audit Logs for each component. Only Super Administrators and System Administrators can review the audit logs.

The TOE provides reliable timestamps to accurately record the sequence of events within the audit records.

b) Cryptographic Support

Forcepoint use FIPS-validated crypto for the protection of sensitive data flows. There are some non-sensitive data flows that leverage crypto that is not FIPS-validated. For example using a MD5 checksum as a network integrity health check. The Forcepoint C Cryptographic Module (CMVP Certificate #2875) is used to protect communications between TOE components, while the Forcepoint Java Cryptographic Module (CMVP Certificate #3113) is used to protect communications between servers and remote management workstations.

c) User Data Protection

The TOE enforces web, data and email filters and policies on user traffic (inbound and/or outbound) to prevents internal entities from accessing potentially harmful or inappropriate content on external data, prevent loss of organisation data and prevent infected email from entering the network. The TOE also supports data classification through the use of the Bolden James tagging system.

d) Identification and Authentication

The TOE enforces identification and authentication for administrators before they can access any management functionality via the CLI or GUI.

The TOE also prevents administrators from accessing FSM and FSAM content before providing and authenticating a valid identity. The TOE maintains a list of security attributes (such as login credentials) for administrators. Authentication can be done either with a username and password or X.509 certificates.

Depending on the web policy applied, unprivileged users are able to browse the internet anonymously.

Email users have to identify and authenticate themselves before the TOE will permit access to their Personal Email Management UI to manage quarantined email messages.

e) Security Management

The TOE provides robust management interfaces that authorized administrators can use to manage the TOE and configure policies to control access to content. By default proxy filtering is enabled, but all traffic is allowed; therefore, the TOE has a permissive default posture.

The TOE defines two categories of administrator — Security Administrator and Delegated Administrator.

System Administrator roles manage system-wide operations, such as setting domains, editing user profiles and permissions, and setting up routes and preferences across all Web, Email, and Data components.

Policy Administrators have custom permission sets defined by associating the Delegated Administrator with one or more roles (set of access privileges) across a single Email, Web and DLP component. For example, a Policy Administrator can be granted "Super Administrator" role in the Web component to manage user profiles, permissions, profiles and settings, similar to a System Administrator role, but limited to only the Web component.

There are eight other permission sets that can be applied to Policy Administrator to manage one or more of the components within FSM.

f) Protection of the TSF

Communications between the DLP Server and DLP endpoints are protected by TLS to protect them from disclosure and modification. This protects the policies that are to be implemented on client devices as well as actions taken by clients as a result of policies being applied. Logical protection of these communications is necessary since DLP endpoints are not co-located with the remainder of the TOE and as such do no benefits from the physical protection of a secure facility.

g) Resource Utilization

The TOE enforces maximum limits on usage and availability of controlled traffic. The TOE is capable of limiting access to specific sites, imposing time constraints on use and capping individual user bandwidth use.

h) TOE Access

The TOE can assign a limit on the number of concurrent sessions that administrative users are allowed to have with FSM. If this limit is reached, the TOE prevents any new sessions from being created.

A FSM console session ends 22 minutes after the last action taken in the user interface (clicking from page to page, entering information, caching changes, or saving changes). A warning message is displayed 5 minutes before session end.

1.4.2 Physical Boundaries

12 The TOE is the On-Premise Security 8.5 solution, including the V-Series appliance on which the Forcepoint Web Security and Forcepoint Email Security components are installed.

13 The other On-Premise Security 8.5 components with the exception of DLP endpoints run on Microsoft Windows Servers and Linux-based soft-appliances.

14 In the evaluated configuration they must be running on Windows Server 2012 or higher.

15 The V-Series appliance hardware is a Dell PowerEdge server with an Intel Xeon processors running a customized version of the CentOS 7 operating system. These comprise the following components:

a) Forcepoint Security Manager 8.5

b) Forcepoint Security Appliance Manager 2.0

c) Forcepoint Web Security Appliance 8.5

d) Forcepoint Email Security Appliance 8.5

e) Forcepoint DLP Server 8.5

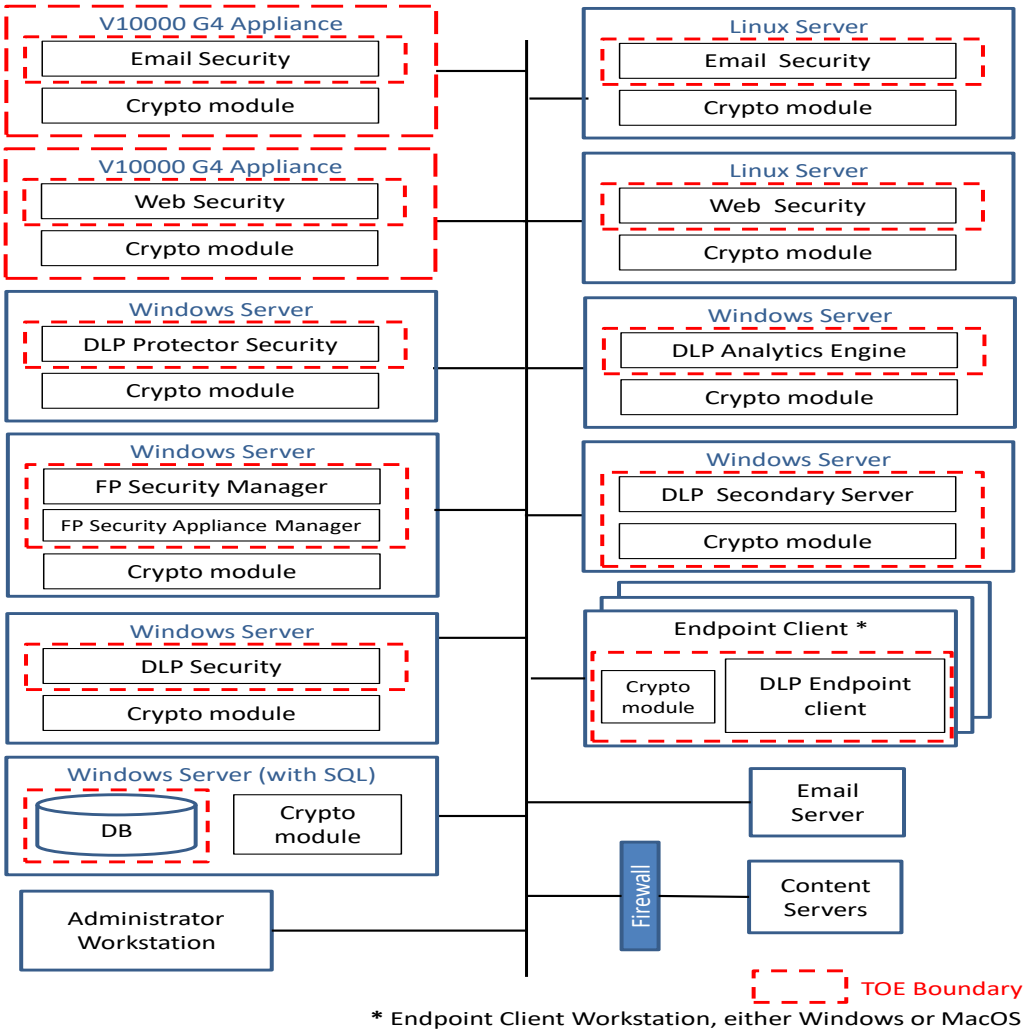
f) Forcepoint DLP Analytics Engine 8.5

g) Forcepoint DLP Endpoint 8.5 (Windows)

h) Forcepoint DLP Endpoint 8.5 (MacOS).

16 In addition to physical platforms, the Analytics Engine, Web Security Appliance and Email Security Appliances can be deployed on virtualized hardware. The TOE supports VMware ESX v6.0. Refer Figure 1 for TOE physical boundary

Figure 1: TOE physical boundary



1.5 Clarification of Scope

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

18 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]).

19 Potential consumers of the TOE are advised that some functions and services of the overall product have not have 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

20 This section summarizes 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 Environmental assumptions

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

a) A.INSTALL

On-Premise Security has been installed and configured according to the appropriate installation guides.

b) A.NETWORK

All policy-controlled traffic between the internal and external networks traverses On-Premise Security.

c) A.LOCATE

It is assumed that the On-Premise Security appliance and associated servers are located within the same controlled-access facility and exclude unauthorized access to the internal physical network.

d) A.NOEVIL

It is assumed that administrators who manage On-Premise Security are not careless, negligent, or wilfully hostile; are appropriately trained; and follow all guidance. Similarly is it assumed that users of the DLP endpoint component are not negligent or wilfully hostile.

e) A. MANAGE

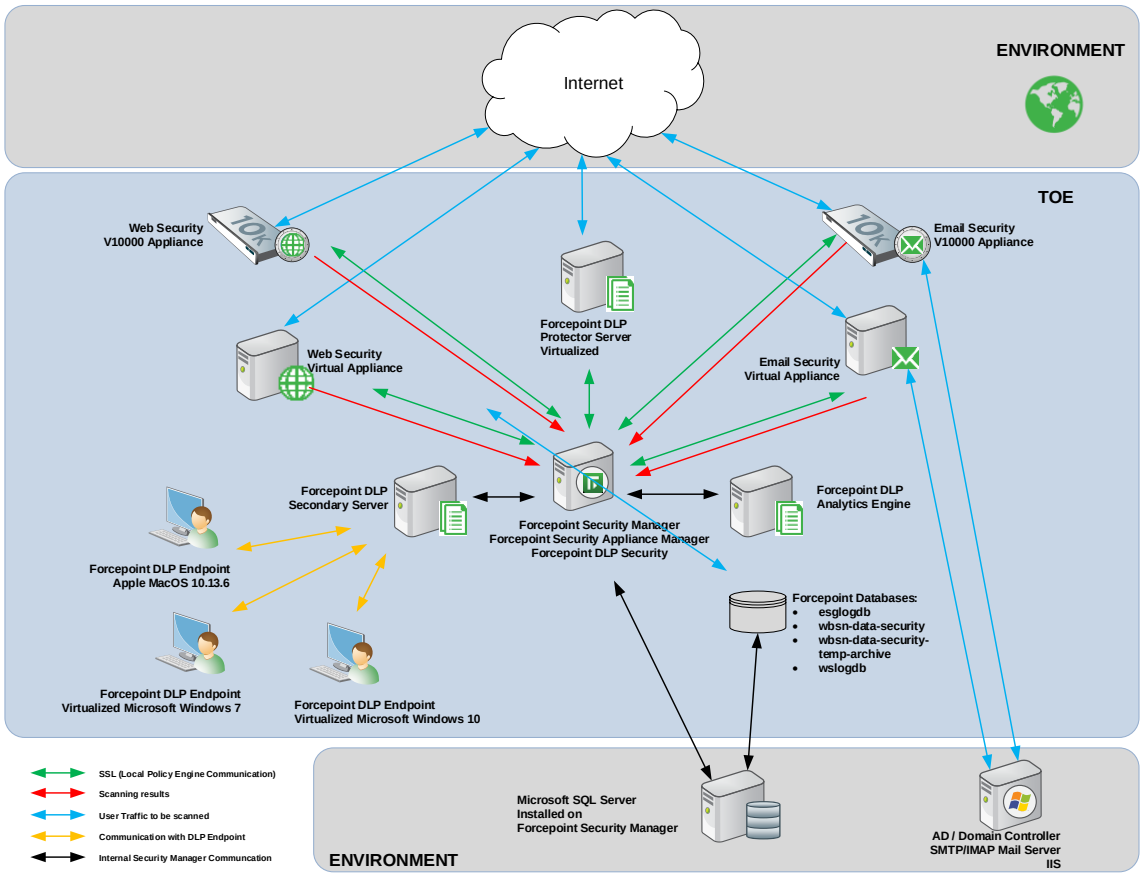
There are one or more competent individuals assigned to manage On-Premise Security and the security of the information it contains.

1.7 Evaluated Configuration

22 The TOE is separated into various subsystems that provide the TOE Security Functions (TSFs).

23 The evaluated configuration of the TOE, shown in Figure 2 is a combination hardware appliance and software application suite that provides email gateway and web scanning services, as well as data loss prevention capabilities.

Figure 2 : Evaluated Deployment Configuration of the TOE



1.8 Delivery Procedures

24 The evaluators examined the delivery procedure, in which provide guidance for the developer to initiate delivery process of the TOE and its components to the intended recipient(s). It is also provide direction on the methods used to deliver the TOE to consumers and users of the product.

25 The TOE consists of both hardware and software. The Email Security and Web Security components are pre-installed on the Forcepoint V10000 G4 Appliance before it is shipped to the customer.

26 The shipping carton contains an appliance (with software image pre-installed), and accessories. The customer can access the TOE software (when logging into their user account at https://support.forcepoint.com/MyAccount) and documentation on the Forcepoint support website (https://support.forcepoint.com/Documentation).

27 Forcepoint uses a third-party company to perform various activities related to delivery of the TOE to the customer, including stocking, manufacturing, testing, quality assurance, integration, logistics, and delivery. This company is referred to as the "Contract Manufacturer."

28 When the customer purchases the V10000 G4 Security Appliance v8.5, all software is pre-installed during manufacturing. All packaging of the TOE is done by the Contract Manufacturer at their factory locations. The carton is labelled with a part number and serial number that can be cross-checked with the BOM.

29 At the factories, a set of employees are conducting quality control inspections of every unit before they are placed into inventory. A different resource reviews each unit a Contract Manufacturer employee creates against the latest BOM to confirm the unit is meeting pre-defined, approved specifications. Inspections are conducted by the Forcepoint Manufacturing Operations Team at irregular intervals and at the executive level quarterly to review the manufacturing process and environment. The inspections ensure that all issues and problems with the packaging and shipping processes are identified and corrected.

30 Shipping of the TOE is managed by Forcepoint in conjunction with the contract manufacturers based on timeline and carrier availability. Common shipping carriers used to ship the TOE to customers are Federal Express (FedEx) and Crane Logistics (Crane). Forcepoint uses the online tracking system of these carriers and provides the information to the purchasing customer via email. The outsourced factories generate daily reports on each shipment. Any shipments that encounter stoppages are immediately investigated.

31 Forcepoint often involves distributors and resellers in purchases. Those organisations will contact the customer directly with delivery information.

32 Customers can verify that they have received the correct hardware product by checking the shipping number on the shipping carton to ensure that it matches the number provided by Forcepoint.

33 The customer can also verify the integrity of the downloaded software by calculating the MD5/SHA256 hash of the downloaded files and comparing them against the hashes posted on the download page for that file.

34 They can also verify the version of the server software clicking the *About* option under the *Help* menu on the Forcepoint Security Manager.

2 Evaluation

35 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 Augmented (ALC_FLR.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

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

2.1.1 Life-cycle support

37 The evaluators checked that the TOE provided for evaluation is labelled with its reference.

38 The evaluators checked that the TOE references used are consistent.

39 The evaluators examined the method of identifying configuration items to determine that it describes how configuration items are uniquely identified.

40 The evaluators examined the configuration items to determine that they are identified in a way that is consistent with the CM documentation.

41 The evaluators checked that the configuration list includes the

a) the TOE itself;

b) the parts that comprise the TOE;

c) the evaluation evidence required by the SARs in the ST

42 The evaluators examined the configuration list to determine that it uniquely identifies each configuration item.

43 The evaluators checked that the configuration list indicates the developer of each TSF relevant configuration item.

2.1.2 TOE Delivery

44 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.

2.1.3 Basic Flaw Remediation

45 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.

46 The evaluator examined the flaw remediation procedures and determined that it describes the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

47 The evaluator examined the flaw remediation procedures and determined that it describes the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users for each of the security flaws.

48 The evaluator examined the flaw remediation procedures and determined that it describes a means by which the developer receives from TOE users' reports and enquiries of suspected security flaws in the TOE.

49 The evaluator examined the flaw remediation procedures and determined that it describes that any reported flaws are remediated and the remediation procedures are issued to TOE users.

50 The evaluator examined the procedures for processing reported security flaws and determined that it provides safeguards that any corrections to these security flaws do not introduce any new flaws.

51 The evaluator examined the flaw remediation guidance and determined that it describes a means by which TOE users report to the developer any suspected security flaws in the TOE.

2.1.4 Development

52 The evaluators examined the security architecture description 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.

53 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.

54 The evaluators examined the functional specification and determined that the TSF is fully represented, it states the purpose of each TSF interface and method of use for each TSFI is given.

55 The evaluators examined the presentation of the TSFI to determine that it completely identifies all parameters associated with every TSFI and completely and accurately describes all error messages resulting from an invocation of each SFR-enforcing TSFI.

56 The evaluators examined the presentation of the TSFI to determine that it completely and accurately describes the SFR-enforcing actions associated with the SFR-enforcing TSFIs.

57 The evaluators examined that the developer supplied tracing links of the SFRs to the corresponding TSFIs.

58 The evaluators examined the TOE design to determine that the structure of the entire TOE is described in terms of subsystems and all subsystems of the TSF are identified.

59 The evaluators examined the TOE and determined that each SFR-non interfering subsystem of the TSF was described such that the evaluators could determine that the subsystem is SFR-non interfering.

60 The evaluators examined the TOE design to determine that it provides a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

61 The evaluators examined the TOE design to determine that it contains a complete and accurate high-level description of the SFR-supporting and SFR-non interfering behaviour of the SFR-enforcing subsystems. The evaluators determined that the TOE design provided a complete and accurate high-level description of the behaviour of the SFR-supporting subsystems.

62 The evaluators examined 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.

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

2.1.5 Guidance documents

64 The evaluators examined the operational user guidance and 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.

65 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.

66 The evaluators examined the provided delivery acceptance and determined that they describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.

67 The evaluators determined that the provided installation procedures describe the steps necessary for secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives in the ST.

68 The evaluators performed all user procedures necessary to prepare the TOE during testing and determined that the TOE and its operational environment can be prepared securely using only the supplied preparative user guidance.

2.1.6 IT Product Testing

69 Testing at EAL 2 Augmented (ALC_FLR.2) consists of assessing developer tests, sufficiency test and conducting penetration tests. The TOE testing was conducted by evaluators from BAE Applied Intelligence MySEF lab. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report.

2.1.6.1 Assessment of Developer Tests

70 The evaluators verified that the developer has met their testing responsibilities by repeating the 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.

2.1.6.2 Independent Test

71 At EAL 2 Augmented (ALC_FLR.2), independent test demonstrates the correspondence between the security functional requirements (SFRs) defined in Security Target, and the test cases that test the functions and behaviour of the TOE that meets those requirements. The evaluators have decided to perform testing based on the TOE Security Functions.

72 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 developed and performed by the evaluators to verify the functionality as follows:

Table 2: Independent Test

Test ID	Description	SFRs	Results
TEST-IND-001-GUI	• Verify that the TSF shall maintain the following list of security attributes belonging to individual administrators. • Verify that all users to be successfully identified and authenticated before allowing any other TSF-mediated actions. • Verify that the TSF is capable of performing management of security functions, security attributes and TSF data. • Verify that the TSF shall maintain the roles and able to associate users with roles. • Verify that the TSF restricts the ability to disable, enable and modify the behaviour of Forcepoint components' functions to authorised users. • Verify that the TSF restricts the capability to specify an expiration time for management session time and terminate the session after the expiration time for the indicated security attribute has passed. • Verify that the TSF provides a reliable time stamp. • Verify that the TSF generates audit records for auditable events and provides a method for authorised users to access all audit data from audit records.	FIA_ATD.1.1, FIA_UAU.1.2, FIA_UAU.2.1, FIA_UID.1.2, FIA_UID.2.1, FMT_SMF.1.1, FMT_SMR.1.1, FMT_SMR.1.2, FMT_MOF.1.1, FMT_SAE.1.2, FTA_SSL.3.1, FPT_STM.1.1, FAU_GEN_EXT.1.1, FAU_GEN_EXT.1.2, FAU_SAR.1.1, FAU_SAR.1.2, FAU_SAR.2.1	Pass

Test ID	Description	SFRs	Results
TEST-IND-002-WEB	• Verify that TSF enforces Internet Access Policy on subjects, objects and operations based on security and object attributes. • Verify that the TSF allows Super administrators and Policy Administrators to specify alternative initial values to override the default values when an object or information is created. • Verify the TSF enforces the policies, allowing the authorised users to change and view the security attributes of the TOE.	FDP_ACC.1.1(a), FDP_ACF.1.1(a), FDP_ACF.1.2(a), FDP_ACF.1.3(a), FDP_ACF.1.4(a), FMT_MSA.1.1(a), FMT_MSA.1.1(b), FMT_MSA.3.1(a), FMT_MSA.3.2(a), FPT_STM.1.1, FPT_ITT.1.1, FAU_GEN_EXT.1.1, FAU_GEN_EXT.1.2, FAU_SAR.1.1, FAU_SAR.1.2, FAU_SAR.2.1	Pass
TEST-IND-003-DLP	• Verify that TSF enforces Data Loss Prevention Policy on subjects, objects and operations based on security and object attributes. • Verify that the TSF allows Super administrators and Policy Administrators to specify alternative initial values to override the default values when an object or information is created. • Verify the TSF enforces the policies, allowing the authorised users to change and view the security attributes of the TOE. • Verify that the TSF data is protected from disclosure and modification when it is transmitted between separate parts of the TOE. • Verify that the TSF provides a reliable time stamp.	FDP_ACC.1.1(b), FDP_ACF.1.1(b), FDP_ACF.1.2(b), FDP_ACF.1.3(b), FDP_ACF.1.4(b), FMT_MSA.1.1(a), FMT_MSA.1.1(b), FMT_MSA.3.1(b), FMT_MSA.3.2(b), FPT_STM.1.1, FPT_ITT.1.1	Pass

Test ID	Description	SFRs	Results
TEST-IND-004-EMAIL	• Verify that TSF enforces Email Policy on subjects, objects and operations based on security and object attributes. • Verify that the TSF allows Super administrators and Policy Administrators to specify alternative initial values to override the default values when an object or information is created. • Verify the TSF enforces the policies, allowing the authorised users to change and view the security attributes of the TOE. • Verify that the TSF data is protected from disclosure and modification when it is transmitted between separate parts of the TOE. • Verify that the TSF provides a reliable time stamp. • Verify that the TSF restrict the ability to query, search, sort, and select the audit data to Super Administrators.	FDP_ACC.1.1(c), FDP_ACF.1.1(c), FDP_ACF.1.2(c), FDP_ACF.1.3(c), FDP_ACF.1.4(c), FMT_MTD.1.1, FMT_MSA.1.1(a), FMT_MSA.1.1(b), FMT_MSA.3.1(c), FMT_MSA.3.2(c), FMT_MTD.1.1, FPT_STM.1.1, FPT_ITT.1.1	Pass
TEST-IND-005-CLI	• Verify that the TSF shall maintain the following list of security attributes belonging to individual administrators. • Verify that all users to be successfully identified and authenticated before allowing any other TSF-mediated actions. • Verify that the TSF data is protected from disclosure and modification when it is transmitted between separate parts of the TOE. • Verify that the TSF provides a reliable time stamp. • Verify that the TSF generates audit records for auditable events.	FIA_ATD.1.1, FIA_UAU.1.1, FIA_UAU.1.2, FIA_UAU.2.1, FIA_UID.1.1, FIA_UID.1.2 FIA_UID.2.1, FPT_STM.1.1, FAU_GEN_EXT.1.1, FAU_GEN_EXT.1.2, FAU_SAR.1.1, FAU_SAR.1.2, FAU_SAR.2.1	Pass

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

2.1.6.3 Vulnerability Analysis

74 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.

75 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks 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 (elapse 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 equipment required for exploitation

2.1.6.3.1 Vulnerability testing

76 The penetration tests focused on:

a) Network vulnerability scan

b) Web vulnerability scan

c) Input data validation

d) Missing function level access control

e) Weak encryption communication channel

f) Unrestricted file upload

77 The results of the penetration testing demonstrate that the TOE is resistant to an attacker possessing a basic attack potential. However, it is important to ensure that the TOE is used only in its evaluated configuration and in a secure environment as specified in the Security Target (Ref [6]). The testing covered the deployment of the TOE on the physical V-series appliances and virtual appliances.

2.1.6.3.2 Testing Results

78 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 the tests conducted were PASSED as expected.

3 Result of the Evaluation

79 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 Forcepoint On-Premise Security 8.5 which is performed by BAE Systems Applied Intelligence MySEF.

80 BAE Systems Applied Intelligence MySEF found that Forcepoint On-Premise Security 8.5 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 (ALC_FLR.2)

81 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

82 EAL 2 Augmented (ALC_FLR.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 and the implementation to understand the security behaviour.

83 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 an attacker possessing a Basic attack potential.

84 EAL 2 Augmented (ALC_FLR.2) also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

85 The Malaysian Certification Body (MyCB) is strongly recommended that:

a) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

b) Potential purchasers of the TOE should ensure that the administrators responsible for the TOE are provided sufficient training and are familiar with the guidance supplements prior to configuring and administering the TOE.

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] Forcepoint On-Premise Security 8.5 Security Target, Version 1.0, 20 May 2019.

[7] Evaluation Technical Report Forcepoint On-Premise Security 8.5, Version 1.1, 24 June 2019.

A.2 Terminology

A.2.1 Acronyms

Table 3: 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
PP	Protection Profile
ST	Security Target

Acronym	Expanded Term
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 4: 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.
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.

Term	Definition and Source
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 ---