MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

# C101 Certification Report

## Cohesity DataPlatform and DataProtect V6.0.1

File name: ISCB-3-RPT-C101-CR-V1
Version: V1
Date of document: 9 August 2019
Document classification: PUBLIC


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

CyberSecurity Malaysia
(726630-U)
T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999

Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

# C101 Certification Report

## Cohesity DataPlatform and DataProtect V6.0.1

9 August 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:*** | C101 Certification Report |
| ***DOCUMENT REFERENCE:*** | ISCB-3-RPT-C101-CR-V1 |
| ***ISSUE:*** | V1 |
| ***DATE:*** | 9 August 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 19 August 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 | 5 August 2019 | All | Initial draft |
| V1 | 9 August 2019 | Page 3, 6, 8, 11, 13, 14 | Added information according to Developers and Evaluator's comment |

# Executive Summary

The Target of Evaluation (TOE) is a software suite that is used to hyperconverge secondary storage workloads (i.e., enterprise data backups) into a single managed backup solution, which may distribute across multiple distributed appliances.

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 with ALC_FLR.1. 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 Systems Lab – MySEF and the evaluation was completed on 29 July 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 Cohesity DataPlatform and DataProtect V6.0.1 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 Cohesity DataPlatform and DataProtect (or collectively simply as "Cohesity"), a software suite that is used to hyperconverge secondary storage workloads (i.e., enterprise data backups) into a single managed backup solution, which may be distributed across multiple distributed appliances. The intent of this product is to simplify the infrastructure and resources used to administer data backup and recovery functions across an enterprise. The TOE natively supports backups for various virtual machines, databases, and network-attached storage (NAS) devices.

2 The TOE also interfaces natively with various cloud service providers for long-term archival and retention of backup data. Backup data stored by the TOE is protected against unauthorized modification and disclosure using symmetric encryption. The TOE provides a role-based access control policy for accessing stored data and administrative functionality.

3 Cohesity is designed to eliminate secondary storage silos by converging all secondary storage and associated data services on one unified solution – including backups, cloud gateway, files, objects, test/dev copies, and data analytics. Cohesity is a software-defined solution that spans from the edge, to the datacenter, and the cloud. With Cohesity, enterprises can:

- Simplify data protection infrastructure by converging legacy backup silos
- Consolidate file and object services
- Build a multicloud data fabric with native cloud integration for archival, tiering and replication
- Accelerate test/dev with copy data management
- Gain visibility into their dark data with in-place analytics
- Reduce total cost of ownership for secondary storage by 50% or more

4 The TOE includes the following security functions:

- Security Audit
- Cryptographic Support
- User Data Protection

- Identification and Authentication
- Security Management
- Self-Protection
- Resource Utilization
- Trusted Communication

## 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** | C101 |
| **TOE Name** | Cohesity DataPlatform and DataProtect |
| **TOE Version** | V6.0.1 |
| **Security Target Title** | Cohesity DataPlatform and DataProtect Security Target |
| **Security Target Version** | v1.0 |
| **Security Target Date** | 15 June 2019 |
| **Assurance Level** | Evaluation Assurance Level 2 Augmented with ALC_FLR.1 |
| **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<br>CC Part 3 Conformant<br>Package conformant to EAL 2 Augmented with ALC_FLR.1 |
| **Sponsor** | Cohesity Inc. |
| **Developer** | Cohesity Inc. |
| **Evaluation Facility** | BAE Systems Lab - MySEF |

## 1.3 Security Policy

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

## 1.4 TOE Architecture

7 The TOE includes both physical and logical boundaries which are described in Sections 2.3 and 2.4 of the Security Target (Ref [6]).

### 1.4.1 Logical Boundaries

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

Table 2: Cohesity DataPlatform and DataProtect Logical Boundaries

| | |
|---|---|
| Security Audit | The TOE generates audits of user activity and security-relevant events that occur on the cluster, such as job failures or disk storage alerts. Audit data is distributed amongst the various nodes in the cluster to ensure that it is replicated. This stored data cannot be modified or deleted by any user or administrator. In the evaluated configuration, the various nodes are configured to send their audit data to a remote syslog server. |
| Cryptographic Support | The TOE supports TLS (independently and as part of HTTPS) and SSH to perform trusted communications. The TOE also uses symmetric cryptography to encrypt backup data at rest. Long-term storage of symmetric keys used to encrypt data at rest is the responsibility of the Operational Environment. Certificate data and short-term keys, such as keys established to enable TLS communications, are zeroized when no longer in use.<br><br>The cryptographic functions used to secure data at rest and in transit are NIST-approved algorithm implementations. |
| User Data Protection | The TOE provides mechanisms for acquiring data from the operational environment for backup purposes. Data can be acquired from various sources such as physical servers, virtual servers, databases, storage arrays, and NAS. While the data is stored internally to the TOE, it may also be |

| | |
|---|---|
| | configured to be viewable as a SMB or NFS storage device. Access controls, both within the TOE's management interfaces and on any SMB/NFS shared data, are used to define the data that can be accessed by TOE and organizational users. Data at rest is protected using AES-256 encryption to prevent unauthorized access.<br><br>The basic functionality for the TOE's data protection function is to back up data from environmental sources, store it within the TOE, and use it to perform restore operations as needed. Data can be set as immutable so that an accurate reversion of working data (such as in the case of a ransomware attack) can be restored to the affected environmental systems. Policies define the data that is acquired as well as the frequency of the backup operations, as well as whether full or incremental backups are performed. Data stored on the TOE may also be sent to a remote Cloud Service Provider or a remote Cohesity Cluster (i.e. a second deployment of Cohesity) for replication or cold storage (archival) purposes.<br><br>The TOE includes an Analytics Workbench application that provides a MapReduce framework for analysis and reporting on data stored within the TOE. This can be used to search for significant data, such as specific text strings/patterns, strings that may be indicative of cleartext passwords, or uncompressed video. Filters can be applied to search parameters so that, for example, data stored in a certain location or that is of a certain age can be excluded from the search. Additional custom searches can be defined by users. |
| Identification and Authentication | The TOE requires user authentication prior to accessing any of its security functionality. This is done using either username/password (for web GUI and SSH), public key authentication (for SSH), or token (for REST API). Username/password data for the web GUI can be defined on the TOE or the TOE can connect to an environmental Active Directory server to perform authentication; the SSH interface uses either AD credentials or locally-defined |

| | |
|---|---|
| | credentials, depending on the functionality that the SSH interface is being used to perform.<br><br>The TOE includes self-signed certificates for its server functionality that are implicitly trusted by the TSF. These can be replaced with user-supplied certificates that are subject to validation, including revocation checking. The TSF also performs certificate validation on server certificates presented to it as part of establishing outbound trusted channels with remote servers such as Active Directory. |
| Security Management | The TSF provides three management interfaces: a web GUI (also known as Cohesity Dashboard), a CLI, and a REST API. The set of management functions available for use to interact with the TSF depends on the interface used to access the TOE.<br><br>The TOE has five defined management roles by default. These roles grant differing degrees of access to the management functionality of the TOE. Additional roles can be defined as needed. Individual users may be restricted in the set of objects that they can perform their assigned management privileges against. |
| Protection of the TSF | The TOE is deployed as a distributed system, which allows for redundant data storage. Redundancy is achieved either through the use of replication factors (i.e. duplicate copies of data stored on different disks/nodes) or erasure coding.<br><br>The TOE performs a series of self-tests when a node is powered on. This includes validation of the cryptographic functionality, which is performed by the Cohesity OpenSSL FIPS Object Module (CMVP certificate #2676). It also includes various boot checks of a node, including correct operation of OS/service boot, storage disks, and network availability. If a node experiences a failure, it will enter a degraded mode of operation and attempt to reboot. The degraded status will be reported to administrators in the management interface. |

| | |
|---|---|
| Resource Utilisation | The TOE provides methods for administrators to configure replication of data across multiple nodes or Cohesity clusters.<br>The TSF also includes a function called 'intelligent data placement' which automatically places data on appropriate nodes based on QoS and IO profiles. This ensures that access to data backup and recovery functions is maintained in the event of the failure/unavailability of individual nodes/disks or in a traffic-constrained environment. |
| Trusted Path/Channels | The TOE uses its FIPS-validated cryptographic module to provide secure communications between itself and remote IT entities/administrators. Specifically, the following interfaces use the following trusted channels/paths:<br>TOE to AD trusted channel – LDAP over TLS<br>TOE to remote CSP trusted channel – TLS/HTTPS<br>TOE to Secondary Cohesity Cluster trusted channel – TLS/HTTPS<br>TOE to Source trusted channel – TLS/HTTPS<br>TOE to Cohesity Analytics – TLS<br>Remote Source to TOE trusted channel – TLS/HTTPS<br>Remote CLI to TOE trusted path – SSH<br>Remote GUI to TOE trusted path – TLS/HTTPS<br>Remote REST API to TOE trusted path – TLS/HTTPS |

### 1.4.2 Physical Boundaries

9 The TOE is installed on a node, which can be any of the physical and/or virtual components listed in Section 2.2 of the Security Target (Ref [6]).

10 The TOE can be deployed on a first-party hyperconverged node or supported third-party hardware, the only system requirement is that a supported hardware model is used. The dedicated hardware used for the TOE is a 2U4N system, which contains four separate nodes within one single 2U chassis, or block.

11 If an instance of the TOE is deployed on a cloud platform, the only system requirement is that Microsoft Azure, AWS, or Google Cloud is the cloud service provider (CSP) that is used. If an instance of the TOE is deployed on a general-purpose computer, that computer must be running CentOS 7.x and have a 64-bit x86 processor architecture. A representative system configuration is provided below—this configuration is identical to the C2105 hyperconverged node sold by Cohesity:

- CPU: Intel Xeon E5-2603 v3
- SATADOM: 8GB
- Memory: 4x16GB
- SSD (for the TOE and its configuration/audit data): 800MB
- HDD (for data backups): 3x2TB
- Network connectivity: 2x1GbE; 2x10GbE

12 While the actual hardware on which the TOE runs is not part of the TOE, the backup data stored on this hardware is considered to be TSF data and therefore protection of it falls within the scope of the TOE.

13 Moreover, the TOE requires the following components in its operational environment to support the enforcement of its security functions:

- Physical/logical storage capable of having backup data ingested by the TSF (also known as Sources) – any of the following are supported:
  - Virtual servers: VMware, Hyper-V, AHV, RHEV
  - Physical servers: Windows, Linux, AIX
  - Applications: Microsoft Exchange
  - Databases: Microsoft SQL Server, Oracle
  - Storage integrations: Pure FlashArray
  - Network Attached Storage: NetApp cluster, Isilon cluster, Pure FlashBlade, generic NFS, SMB
  - Cohesity Agent: installed on the following Sources to provide an interface to transfer data from that Source to the TOE:
  - Virtual servers: Hyper-V (or SCVMM server containing multiple Hyper-V VMs), VMware, AHV, RHEV
  - Physical Servers: all

- Databases: all
    - Web browser with HTML5 support (for administration)
    - SSH client (for administration)
    - KMIP-compliant Key Manager (for management and secure storage of KEKs)

14 The TOE may or may not make use of the following environmental components, depending on how it is configured:

- VMware vSphere (5.5 or higher) or Microsoft Hyper-V server (2012 or 2016): required if Cohesity Virtual Edition is used
- Active Directory: optional for authentication and authorization
- DNS Server: optional for use of name services
- NTP Server: optional for use of network time
- Syslog Server: optional for remote storage of audit data
- Cloud Service Providers (Microsoft Azure, AWS, Google Cloud, Oracle, or any S3 compatible private cloud or on premise object storage): optional for use of cloud backup
- External Cohesity Cluster: optional for replication of stored data
- Cohesity Analytics: optional service run by Cohesity for remote telemetry and support automation

## 1.5 Clarification of Scope

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

16 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]).

17 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.

18 The following capabilities are part of the Cohesity product but excluded from the evaluated configuration because they prevent the TSF from being fully implemented:

- DataPlatform standalone configuration: DataPlatform does not require DataProtect to be present to function, but DataProtect is required for the evaluated configuration in order to provide the security functionality claimed in this ST.
- Internal key manager: Cohesity provides its own key management capability for storage of DEKs, but access to the KEKs used to encrypt the DEKs is controlled through logical access and not a cryptographically-protected REK. Therefore, it is necessary to use a third-party key manager to ensure an appropriate degree of security for the protected data.
- OS root user: Cohesity provides a CLI application, web-based GUI, and REST API to perform security-relevant management functions. By default, Cohesity is installed on a general-purpose operating system by a root-level user account. The root user can perform certain debug-related activities against Cohesity that are not available through any of the TSF-relevant management interfaces. However, these activities are entirely debug-related in nature and will not be invoked when the TOE is operating properly in its evaluated configuration.

## 1.6 Assumptions

19 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

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

Table 3: Assumptions for the TOE environment

| Assumption | Statements |
|---|---|
| A.COMPONENTS RUNNING | It is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack or failure of one or more of the TOE components. |

| Assumption | Statements |
|---|---|
| A.LIMITED | It is assumed that the hardware components that comprise the TOE are used only for the functionality provided by the TSF and that the TOE does not include any other general-purpose computing capabilities that present additional external interfaces to the TSF. |
| A.NETWORK | It is assumed that the nodes on which the TOE is deployed are connected to one another over a local network that is not subject to unauthorized surveillance. |
| A.PHYSICAL | It is assumed that the TOE is deployed in a location that is physically secured in its operational environment and not subject to any attacks on the physical interfaces of the TOE or the TOE hardware itself. |
| A.REGULAR UPDATES | It is assumed that TOE software/firmware updates are applied on a regular schedule and/or within a reasonable period of time after they have been made available by the vendor. |
| A.SYSTEM TIME | The TOE's operational environment is assumed to provide reliable system time for all nodes. |
| A.TRUSTED ADMIN | It is assumed that any administrators of the TOE are trusted to be technically competent, non-malicious, and to follow operational and preparatory guidance as directed for the functions that they are authorized to perform. |

## 1.7 Evaluated Configuration

21 The TOE may be deployed in a number of configurations consistent with the requirements identified in this Security Target (Ref [6]). The TOE boundary includes the DataPlatform and DataProtect software installed on a node. A node may contain multiple individual storage disks, and a combination of nodes is referred as a cluster. In the evaluated configuration, both TOE components are present on each node, and the components are:

- Cohesity DataPlatform – a software-defined, web-scale platform used to consolidate secondary data
- Cohesity DataProtect – a converged backup and recovery solution that runs on DataPlatform

22 Administration of the TOE is performed using SSH and Web GUI components that are part of DataProtect. When operating in a cluster (multiple distributed nodes), a single node is designated as the primary node, and this node is used to administer the entire cluster. The TOE supports the following components in the operational environment for the evaluated configuration.

- VMware vSphere (5.5 or higher) or Microsoft Hyper-V server (2012 or 2016) – required if Cohesity Virtual Edition is used.
- Active Directory for authentication and authorisation
- DNS Server for use of name services
- NTP Server for use of network time
- Syslog Server for remote storage of audit data
- External Cohesity Cluster for replication of stored data

23 The following figure shows an example deployment of the TOE in its operational environment.

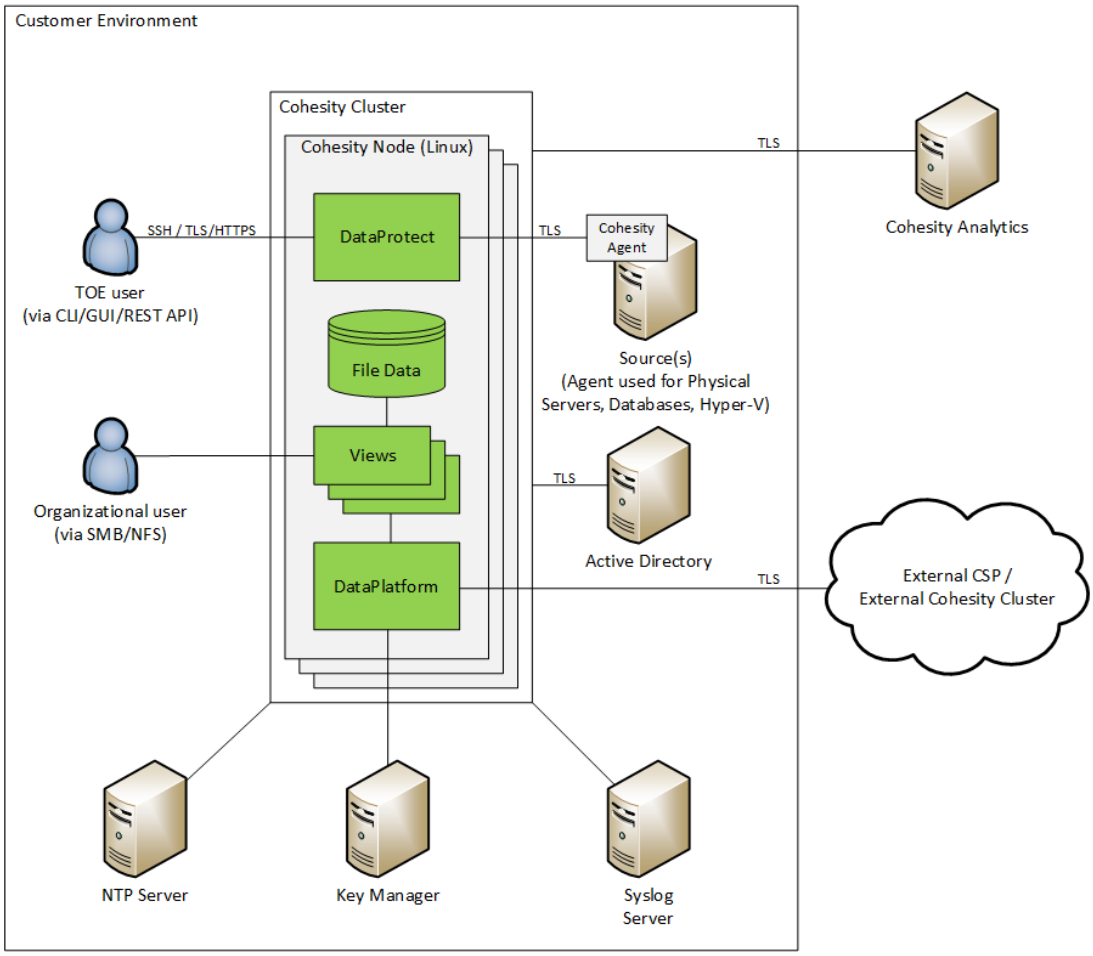


Figure 1: Example TOE Deployment

## 1.8 Delivery Procedures

24 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.

### 1.8.1 Product Orders

25 The customer gets to know about Cohesity Product either through marketing campaign, or partner involvement. Sales Engineers also contact customers on what Cohesity products can do and get them interested to try and buy the products. When a customer is interested to purchase the product, the sales team get involved and go through the procurement process.

### 1.8.2 TOE Delivery

*1.8.2.1 Software Delivery*

26 TOE software is securely delivered from an online portal protected by username/password. The software itself is digitally signed using MD5 checksum and all the RPMs within the packaged software are protected as well using hashes. When there is a new release of the software, email notification is sent to the customer and also the online portal is updated with the new information (link and version). All the manuals associated with the software are also linked to the online portal.

*1.8.2.2 Hardware Delivery*

27 The TOE is a software application that that can be scaled across physically distributed nodes. Customer orders the hardware components via a reseller.

28 Once order is received, ship notification is sent via email. A packing slip on box with model number and serial number matching the packing slip to hardware is sent to the customer. Product name on physical packaging and physical chassis includes top level hardware extended SKU configuration, i.e. C2605-SFP-BASE-4 on a bar coded label and model number on the compliance tick label. Interactive setup/installation materials include high level SKU depending on platform and NIC configuration. There are 3 options - "C2000 Series" for SFP, "C2000 Series RJ45" and "C3500".

29 Hardware components could include shrink-wrapped packaging or security tape. Cartons are shipped and sealed with paper gummed tape and shrink wrapped for cosmetic protection. Cartons have Cohesity logo in black on each side.

## 1.9 Basic Flaw Remediation

30 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.

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

32 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.

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

34 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.

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

# 2 Evaluation

37 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 with ALC_FLR.1. 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

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

### 2.1.1 Life-cycle support

39 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.

40 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 the Security Target (Ref [6]).

41 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

42 The evaluators analyzed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality interfaces (TSFIs), and how the TOE security function (TSF) implements the security functional requirements (SFRs).

43 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined

that, it provides a complete, accurate, and high-level description of the SFR-enforcing behavior of the SFR-enforcing subsystems.

44 The evaluators examined the TOE security architecture description; they 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.

45 At the end, the evaluators confirmed that all the requirements for this class were fulfilled and passed.

### 2.1.3 Guidance documents

46 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

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

### 2.1.4 IT Product Testing

48 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 BAE Systems Lab – MySEF. 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*

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

*2.1.4.2 Independent Functional Testing*

50 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.

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

Table 4: Independent Functional Test

| Test ID | Description | Results |
|---|---|---|
| TEST-IND-001-Web GUI | • To test that the TOE generates audit records and prevents unauthorised deletion to the stored audit records.<br>• To test the TOE identification and authentication process.<br>• To test whether the TSF data is protected from disclosure or modification when it is transmitted between separate parts of the TOE.<br>• To test the TOE's access control functions, user data protection, and security management function behaviors. | Passed. Result as expected. |

| Test ID | Description | Results |
|---|---|---|
| TEST-IND-002-CLI | • To test the TOE's SSH protocol, subset access control, and access control functions.<br>• To test the TOE identification and authentication process.<br>• To test whether the TSF data is protected from disclosure or modification when it is transmitted between separate parts of the TOE.<br>• To test the TOE management functionalities.<br>• To test TOE security function self-test and fault tolerance degradation. | Passed. Result as expected. |
| TEST-IND-003-REST API | • To test the TOE authentication process and security roles.<br>• To test that only authorised users are able to configure and perform TOE security management functions.<br>• To test that the TOE generates audit records. | Passed. Result as expected. |

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

*2.1.4.3 Penetration testing*

53 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.

54 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 (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 requirement for exploitation

55 The penetration tests focused on:

a) General network vulnerability scan;

b) Common web vulnerability scan;

c) Broken Authentication Attack;

d) Input and data validation (GUI);

e) Input and data validation (REST API);

f) Insecure Communication.

56 The result of the penetration testing noted that there is no residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment as specified in Section 4 of the Security Target (Ref [6]).

*2.1.4.4 Testing Results*

57 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 test conducted were PASSED as expected.

# 3 Result of the Evaluation

58 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 Cohesity DataPlatform and DataProtect V6.0.1 which is performed by BAE Systems Lab – MySEF.

59 BAE Systems Lab – MySEF found that Cohesity DataPlatform and DataProtect V6.0.1 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.

60 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

61 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 and the implementation to understand the security behaviours.

62 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.

63 EAL 2 Augmented with ALC_FLR.1 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

## 3.2 Recommendation

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

a) The users should make themselves familiar with the developer guidance provided with the TOE, pay attention to all security warnings as well as to observe the

operational environment requirements and assumptions defined in the applicable Security Target (Ref [6]).

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 System Administrator should review the audit trail generated and exported by the TOE periodically.

# 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] Cohesity DataPlatform & DataProtect Version 6.0.1 Security Target, Version 1.0, 15 June 2019.

[7] Cohesity DataPlatform & DataProtect Version 6.0.1, Evaluation Technical Report, Version 1.0, 29 July 2019.

## A.2 Terminology

### A.2.1 Acronyms

Table 5: List of Acronyms

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

| Acronym | Expanded Term |
|---|---|
| ST | Security Target |
| TOE | Target of Evaluation |

### A.2.2 Glossary of Terms

Table 6: Glossary of Terms

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

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

--- END OF DOCUMENT ---