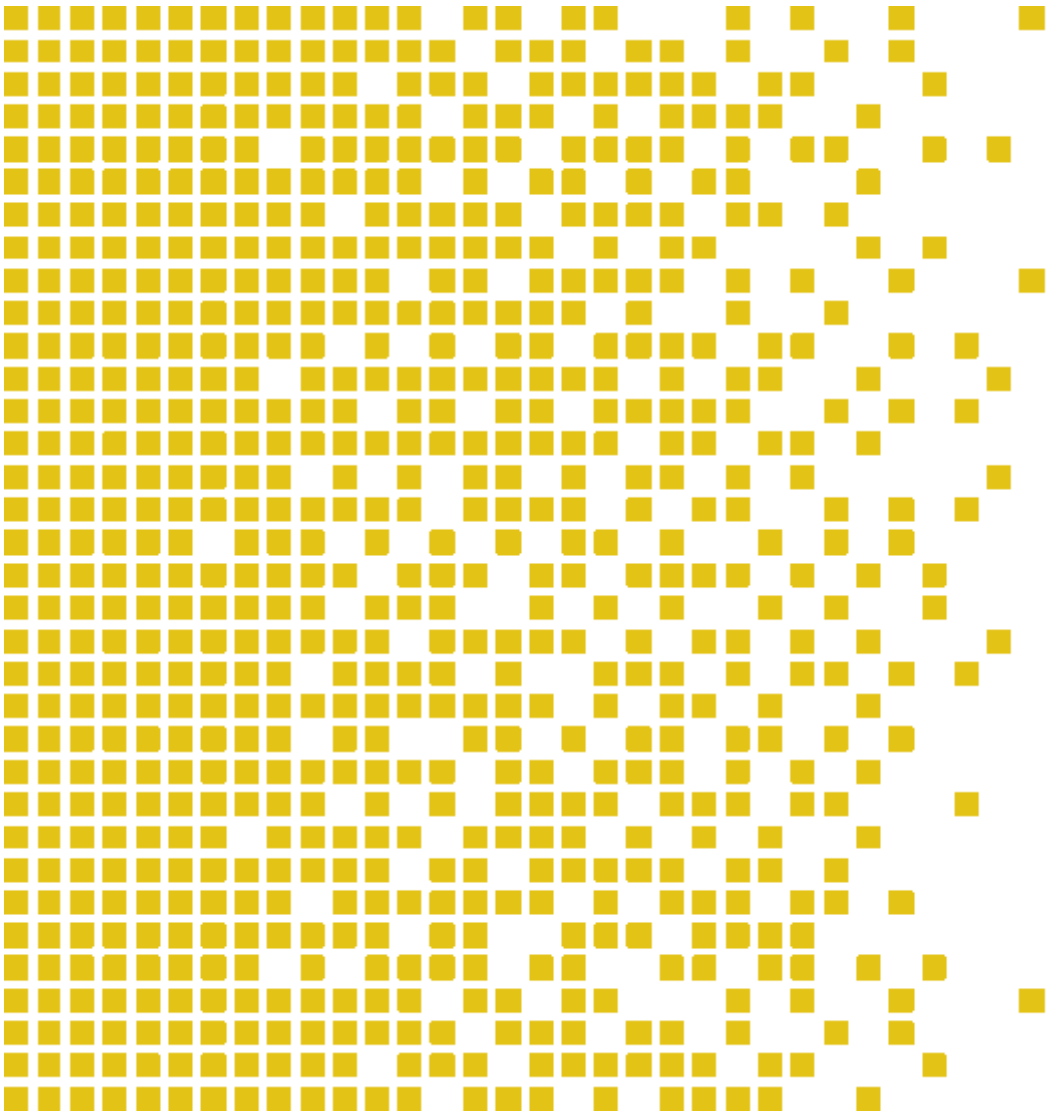
SERTIT-095 CR Certification Report

Issue 1.0 6 Nov 2017

Cisco HyperFlex Systems HX Series v2.5(1c)



SERTIT, Postboks 814, 1306 Sandvika, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Sec urity, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognized under the terms of the CCRA July 2nd 2014.

The recognition under CCRA is limited to cPP related assurance packages or EAL 2 and ALC_FLR CC part 3 components.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Agreement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Agreement and is the Party's claim that the certificate has been issued in accordance with the terms of this Agreement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Mutual recognition under SOGIS MRA applies to components up to EAL 4.

Contents

1 Certification Statement

Cisco Systems, Inc. Cisco HyperFlex Systems HX Series is a hyper-convergent software-centric solution that tightly integrates computing, storage, networking and virtualization resources in a single hardware platform.

Cisco HyperFlex Systems HX Series version v2.5(1c) have been evaluated under the terms of the Norwegian Certification Scheme for IT Security and have met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL 2 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality in the specified environment when running on the platforms specified in Annex A.

Author	Kjartan Jæger Kvassnes Certifier
Quality Assurance	Arne Høye Rage Quality Assurance
Approved	Jørn Arnesen Head of SERTIT
Date approved	6 Nov 2017

2 Abbreviations

AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
API	Application Programming Interface
CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM Evaluation	Common Methodology for Information Technology Security
CIMC	Cisco Integrated Management Controller
CIM-XML	Common Information Model XML
CLI	Command Line Interface
CM	Configuration Management
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
FC	Fibre Channel
HDD	Hard-disk drives
HTTPS	Hyper-Text Transport Protocol Secure
IP	Internet Protocol
OS	Operating System
POC	Point of Contact
QP	Qualified Participant
SAR	Security Assurance Requirement
SERTIT	Norwegian Certification Authority for IT Security
SFP	Security Functional Policy
SFR	Security Functional Requirement

SM	Service Module
SPM	Security Policy Model
SSD	Solid-state disk
SSL	Secure Socket Layer
ST	Security Target
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
UCS	[Cisco] Unified Computing System
UCSM	UCS Manager
UDP	User datagram protocol
VIB	VMware ESXi vSphere Installation Bundles
VLAN	Virtual Local Area Network
VM	Virtual Machine, a virtualized guest operating system installed to a hypervisor.
VMM	Virtual Machine Manager, a hypervisor.
VSAN	Virtual Storage Area Network
XML	Extensible Markup Language

3 References

[1] Security Target, Cisco Systems, Inc., Cisco HyperFlex Systems HX Series Common Criteria Security Target, v1.0, 21 September 2017.

[2] Common Criteria Part 1, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[3] Common Criteria Part 2, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[4] Common Criteria Part 3, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[7] Evaluation Technical Report Common Criteria EAL2 Evaluation of Cisco HyperFlex Systems HX Series v1.0, 29 September 2017.

[8] Cisco HyperFlex Systems HX Series Common Criteria Operational User Guidance and Preparative Procedures, Version 1.0.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Cisco HyperFlex Systems HX Series version v2.5(1c) to the Sponsor, Cisco Systems, Inc., and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The version of the product evaluated was Cisco HyperFlex Systems HX Series and version v2.5(1c).

These products are also described in this report as the Target of Evaluation (TOE). The developer was Cisco Systems, Inc.

The TOE is a hyper-convergent software-centric solution that tightly integrates computing, storage, networking and virtualization resources in a single hardware platform.

The TOE is installed in a hypervisor environment, such as VMware vSphere. The TOE manages the storage of a storage cluster that has a minimum three servers (HyperFlex HX Series Nodes (Converged Host)) with Solid-state disk (SSD) and Hard-disk drives (HDD) attached storage. The clustered servers are networked with switches and fabric interconnects. Optionally, non-storage servers, (compute nodes), can be included in the storage cluster. HX Data Platform manages the storage for the data and VMs stored on the associated storage cluster.

The HyperFlex HX Series installer is loaded on a UCS platform that is networked to the storage cluster to be managed. During the installation of the TOE, the initial cluster with at least three HyperFlex HX Series Nodes is created. The datastores are added to the storage cluster after the installation is complete. The HyperFlex HX Series provides a highly fault-tolerant distributed storage system that preserves data integrity and optimizes performance for virtual machine (VM) storage workloads.

The HyperFlex HX Series includes CLI commands that are used to monitor and manage the storage clusters. The CLI also provides the Authorized Administrator the ability to add nodes as the storage capacity and the storage needs grow within the organization.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

The TOE scope is described in the ST[1], chapter 1.5 and 1.6.

4.4 Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.

4.5 Assurance Level

The Security Target[1] specified the assurance requirements for the evaluation. Predefined evaluation assurance level EAL 2 was used. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

There are no Organizational Security Policies or rules with which the TOE must comply.

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats which these objectives counter and security functional requirements and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered

- **T.ACCOUNTABILITY**
  An authorized administrative is not held accountable for their actions on the TOE because the audit records are not generated or reviewed.
- **T.NOAUTH**
  An unauthorized person (attacker) may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE to disrupt operations of the TOE.
- **T.RESOURCE_AVAILABILITY**
  The TOE data (user) could become corrupted or unavailable due to hardware or system operation failures.
- **T.TIME**
  Evidence of a compromise by an unauthorized user (attacker) or malfunction of the TOE may go unnoticed or not be properly traceable if recorded events (audit data) are not properly sequenced through application of correct timestamps.

4.9 Threats Countered by the TOE's environment

There are no threats countered by the TOE´s environment.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

- **A.ADMIN**
  All Authorized Administrator are assumed not evil, will follow the administrative guidance and will not disrupt the operation of the TOE intentionally.
- **A.CONNECTIONS**
  The operational environment in which the TOE is installed will allow the users of the TOE to access the stored information.
- **A.LOCATE**
  The processing resources of the TOE and those services provided by the operational environment will be located within controlled access facilities, which will prevent unauthorized physical access.

4.12 IT Security Objectives

- **O.ACCESS_CONTROL**
  The TOE will restrict access to the TOE management functions to the Authorized Administrator.
- **O.ADMIN**
  The TOE will provide the Authorized Administrator with a set of privileges to isolate administrative actions and to make the administrative functions available remotely.
- **O.AUDIT_GEN**
  The TOE will generate audit records that will include the time that the event occurred, the identity of the user performing the event and the outcome of the event.
- **O.AVAILABILITY**
  The TOE will provide mechanisms to maintain a secure state and mitigate against data loss or corruption due to hardware or system operation failures.
- **O.AUDIT_VIEW**
  The TOE will provide the Authorized Administrator the capability to review audit data.
- **O.DATA**
  The TOE will protect the configuration and user data from unauthorized modifications.
- **O.IDAUTH**
  The TOE must uniquely identify and authenticate the claimed identity of all administrative users before granting management access.
- **O.SELFPRO**
  The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

- **O.TIME**
  The TOE will provide a reliable time stamp for its own use.

4.13 Non-IT Security Objectives

- **OE.ADMIN**
  The Authorized Administrator are well trained and trusted to manage the TOE and to configure the IT environment and required non-TOE devices for the proper network support.
- **OE.CONNECTION**
  The operational environment will have the required protected network support for the operation of the TOE to prevent unauthorized access to the TOE.
- **OE.LOCATE**
  The processing resources of the TOE and those services provided by the operational environment will be located within controlled access facilities, which will prevent unauthorized physical access.

4.14 Security Functional Requirements

- FAU_GEN.1 Audit data generation
- FAU_GEN.2 User Identity Association
- FAU_SAR.1 Audit Review
- FAU_STG.1 Protected audit trail storage
- FDP_ACC.2 Complete access control
- FDP_ACF.1 Security attribute based access control
- FIA_ATD.1 User Attribute Definition
- FIA_SOS.1 Verification of secrets
- FIA_UAU.2 User Authentication Before Any Action
- FIA_UAU.7 Protected authentication feedback
- FIA_UID.2 User Identification Before Any Action
- FMT_MSA.1 Management of security attributes
- FMT_MSA.3 Static attribute initialization
- FMT_MTD.1 Management of TSF Data
- FMT_SMF.1 Specification of Management Functions
- FMT_SMR.1 Security Roles
- FPT_FLS.1 Failure with preservation of secure state
- FPT_STM.1 Reliable time stamps
- FRU_FLT.2 Limited fault tolerance
- FTA_SSL.3 TSF-initiated termination
- FTP_TRP.1 Trusted path

4.15 Security Function Policy

The TOE is a hyper-convergent software-centric solution that tightly integrates computing, storage, networking and virtualization resources in a single hardware platform.

The TOE is installed in a hypervisor environment, such as VMware vSphere. The TOE manages the storage of a storage cluster that has a minimum three servers (HyperFlex HX Series Nodes (Converged Host)) with Solid-state disk (SSD) and Hard-disk drives (HDD) attached storage. The clustered servers are networked with switches and fabric interconnects. Optionally, non-storage servers, (compute nodes), can be included in the storage cluster. HX Data Platform manages the storage for the data and VMs stored on the associated storage cluster.

The HyperFlex Systems HX Series provides connectivity and security services onto a single, secure device. The TOE offers:

- Enterprise-class data management features that are required for complete lifecycle management and enhanced data protection in distributed storage
- Simplified data management that integrates storage functions into existing management tools and allowing instant provisioning for dramatically simplified daily operations
- Independent scaling of the computing, caching, and capacity tiers, giving you the flexibility to scale the environment based on evolving business needs
- Continuous data optimization with inline data deduplication and compression that increases resource utilization with more headroom for data scaling
- Dynamic data placement in node memory, enterprise-class flash memory (on solid-state disk [SSD] drives), and persistent storage tiers (on hard-disk drives [HDDs]) to optimize performance and resiliency—and to readjust data placement as you scale your cluster

The HyperFlex Systems HX Series delivers the combination of the essential features in a single solution.

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Brightsight B.V. Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[7] to SERTIT in 11 October, 2017. SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3[4]. These classes comprise the EAL 2 assurance package.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Functional specification with complete summary
	ADV_TDS.1	Architectural design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Production support, acceptance procedures and automation
	ALC_CMS.2	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Analysis of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

All assurance classes were found to be satisfactory and were awarded an overall “pass” verdict.

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to

either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the guidance listed in the ST[1] chapter 1.5 provided by the developer. The Operational User Guidance and Preparative Procedures [8] describes all necessary steps to configure the TOE in the certified configuration.

These documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner.

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. The user should always follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

The evaluator while performing other evaluation activities (ASE, ADV and AGD) considered direct attacks, monitoring and misuse attacks, to identify potential vulnerabilities.

The evaluator also, conducted a public domain vulnerability search to further search for potential vulnerabilities. Both TOE specific and TOE type search terms were used. The evaluator also used a vulnerability scanning tool (Nessus) to identify potential vulnerabilities.

The evaluator assessed all possible vulnerabilities found during evaluation. Potential vulnerabilities were found however none of them turned out to be possibly exploitable.

5.6 Developer's Tests

The developer test plan covers all of the security functions listed in the Security Target [1]. This has been achieved by combining where possible, multiple SFRs into a single test case. There are a total of 9 test cases that cover all of the TSFIs and SFRs.

The developer has performed testing on the HyperFlex HX220c M4 Nodes.

5.7 Evaluators' Tests

The evaluator decided to sample based on test cases that covered the majority of SFRs and TSFIs and came up with 3 repeated tests. Furthermore the evaluator analysed the developer test plan to see whether additional ATE tests could be performed, and devised 9 additional tests.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Cisco HyperFlex Systems HX Series version v2.5(1c) meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 2 for the specified Common Criteria Part 2 conformant functionality, in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of Cisco HyperFlex Systems HX Series version v2.5(1c) should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under Section 4.3 “TOE Scope” and Section 5 “Evaluation Findings”.

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

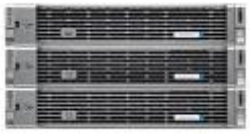
Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

Hardware:

Hardware	Picture	Size	Power	Interfaces
Cisco HyperFlex HX220c M4 Node		**Height** 1.7 in. (4.32 cm) **Width** 16.89 in. (43.0 cm) including handles: 18.98 in. (48.2 cm) **Depth** 29.8 in. (75.6 cm) including handles: 30.98 in. (78.7 cm)	Two 770 W (AC) hot swappable power supplies	**Rear panel** • One DB15 VGA connector • One RJ45 serial port connector • Two USB 3.0 port connectors • One RJ-45 10/100/1000 Ethernet management port, using Cisco Integrated • Management Controller (CIMC) firmware • Two Intel i350 embedded (on the motherboard) GbE LOM ports • One flexible modular LAN on motherboard (mLOM) slot that • Accommodates the Cisco UCS VIC1227 VIC MLOM - Dual Port 10Gb SFP+ interface card. • Two PCIe 3.0 slots **Front panel** • One KVM console connector (supplies two USB 2.0 connectors, one VGA • DB15 connector, and one serial port (RS232) RJ45 connector)

Hardware	Picture	Size	Power	Interfaces
Cisco HyperFlex HX240c M4 Node		Height 3.43 in. (8.70 cm) Width (including slam latches) 17.65 in.(44.8 cm) Including handles: 18.96 in (48.2 cm) Depth 29.0 in. (73.8 cm) Including handles: 30.18 in (76.6 cm)	Up to two hot-pluggable, redundant 650W, 930W DC, 1200W, or 1400W power supplies	**Rear panel** • One DB15 VGA connector • One RJ45 serial port connector • Two USB 3.0 port connectors • One RJ-45 10/100/1000 Ethernet management port, using Cisco Integrated • Management Controller (CIMC) firmware • Two Intel i350 embedded (on the motherboard) GbE LOM ports • One flexible modular LAN on motherboard (mLOM) slot that • Accommodates the Cisco UCS VIC1227 VIC MLOM - Dual Port 10Gb SFP+ interface card. • Two PCIe 3.0 slots **Front panel** • One KVM console connector (supplies two USB 2.0 connectors, one VGA • DB15 video connector, and one serial port (RS232) RJ45 connector)

Hardware	Picture	Size	Power	Interfaces
Cisco HyperFlex HX240c M4 Nodes with Cisco UCS B200 Blade Servers		Same as above for the node and the following blade size Height 1.95 in. (50 mm) Width 8.00 in.(203 mm) Depth 24.4 in. (620 mm)	Same as above for the node and blade	Same as above for the node and the following blade interface: Front panel • One console connector

Software:

- Cisco HyperFlex HX Data Platform Software, version 2.5(1c)

Guidance:

- Cisco HyperFlex Systems HX Series Common Criteria Operational User Guidance and Preparative Procedures, v1.0, 11 October 2017

TOE Documentation

The supporting guidance documents evaluated were:

[a] Cisco HyperFlex Systems HX Series Common Criteria Operational User Guidance and Preparative Procedures, v1.0, 11 October 2017

Further discussion of the supporting guidance material is given in Section 5.3 “Installation and Guidance Documentation”.

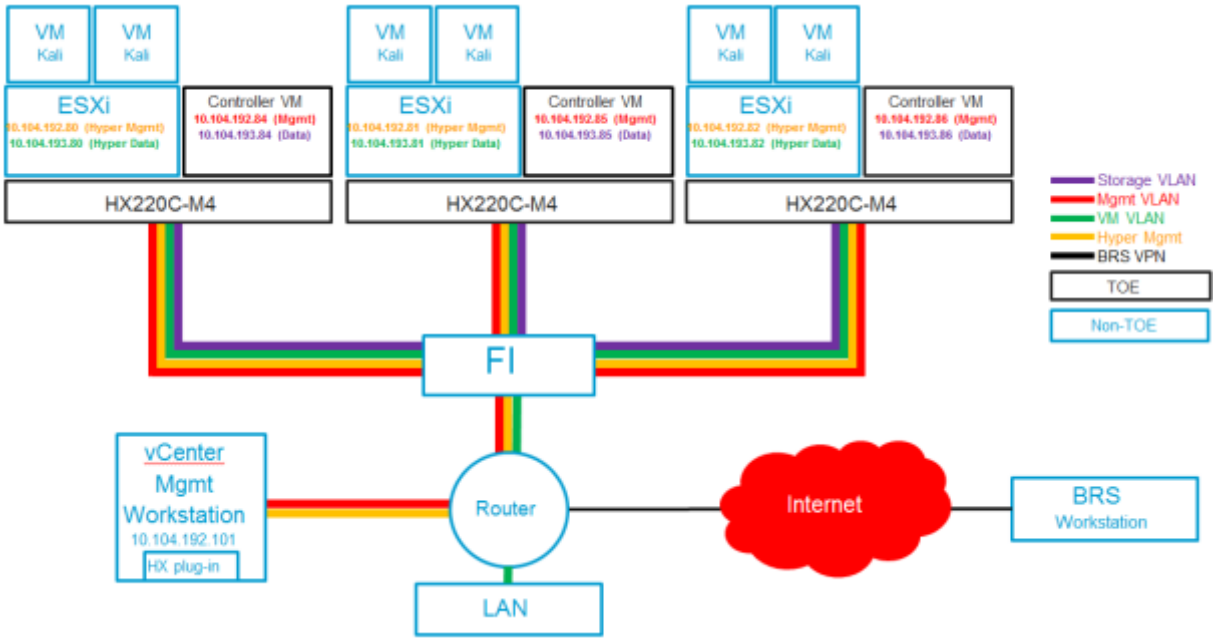
TOE Configuration

The following configuration was used for testing:

The TOE was tested on the following models: HX220c M4 Nodes and HX240c M4 nodes, with Cisco HyperFlex HX Data Platform Software, version 2.5(1c), configured according to [8].

Environmental Configuration

The TOE is tested in the following setup:



Where FI is the Fabric Interconnect of the Cisco UCS which provides connection to the TOE.