# National Information Assurance Partnership
# Common Criteria Evaluation and Validation Scheme



# Validation Report

# Infinera Corporation Transcend Network Management System Server 18.10.3

**Report Number:**      **CCEVS-VR-11319-2022**
**Dated:**      **December 12, 2022**
**Version:**      **1.0**

National Institute of Standards and Technology      Department of Defense
Information Technology Laboratory      ATTN: NIAP, Suite 6982
100 Bureau Drive      9800 Savage Road
Gaithersburg, MD  20899      Fort Meade, MD 20755-6982

# ACKNOWLEDGEMENTS

## <u>Validation Team</u>

## <u>Common Criteria Testing Laboratory</u>

# Table of Contents

# List of Tables

# 1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of Infinera Transcend Network Management System Server solution provided by Infinera Corporation. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in December 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended and meets the assurance requirements of the Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14) with the Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11) and the Functional Package for SSH, Version 1.0, 13 May 2021 (SSH10).

The Target of Evaluation (TOE) is the Infinera Corporation Transcend Network Management System Server 18.10.3. The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Infinera Corporation Transcend Network Management System Server 18.10.3 Security Target, version 1.5, December 9, 2022 and analysis performed by the Validation Team.

# 2   Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

| Item | Identifier |
| --- | --- |
| **Evaluation Scheme** | United States NIAP Common Criteria Evaluation and Validation Scheme |
| **TOE** | Infinera Transcend Network Management System Server 18.10.3 |
| **Protection Profile** | Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14) with the Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11) and the Functional Package for SSH, Version 1.0, 13 May 2021 (SSH10) |
| **ST** | Infinera Corporation Transcend Network Management System Server 18.10.3 Security Target, version 1.5, December 9, 2022 |
| **Evaluation Technical Report** | Evaluation Technical Report for Infinera Corporation Transcend Network Management System Server 18.10.3, version 0.3, December 9, 2022 |
| **CC Version** | Common Criteria for Information Technology Security Evaluation, Version 3.1, Rev 5 |
| **Conformance Result** | CC Part 2 Extended, CC Part 3 Extended |
| **Sponsor** | Infinera Corporation |
| **Developer** | Infinera Corporation |
| **Common Criteria Testing Lab (CCTL)** | Gossamer Security Solutions, Inc. Columbia, MD |
| **CCEVS Validators** | Sheldon Durrant, Lauren Hardy, Randy Heimann, Linda Morrison, Clare Parran, Anne Gugel, Farid Ahmed, Michael Smeltzer, Russel Fink, Richard Toren |

**Table 1: Evaluation Identifiers**

# 3  Assumptions & Clarification of Scope

*Assumptions*
The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14)

- Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11)

- Functional Package for SSH, Version 1.0, 13 May 2021 (SSH10)

That information has not been reproduced here and the ASPP14/PKGTLS11/SSH10 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the ASPP14/PKGTLS11/SSH10 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

*Clarification of scope*
All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the Application Software Protection Profile with the TLS Package and SSH Package and performed by the evaluation team).

- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.

- Apart from the Admin Guide, additional customer documentation for the specific Software Application models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

- The functionality evaluated is scoped exclusively to the security functional requirements specified in the ASPP14/PKGTLS11/SSH10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

# 4  Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Transcend Network Management System (TNMS) is designed to provide end-to-end network and service management across multiple technologies and equipment vendors.  For purposes of this evaluation, the TNMS Server is a software application that accepts management instructions via secure communication with a TNMS Client and then securely transfers management instructions to configured network entities.

Note that the full TNMS system consists of client and server components, this evaluation is limited only to the server components since the Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14) does not support the evaluation of distributed application solutions.

## 4.1  TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 7 below.
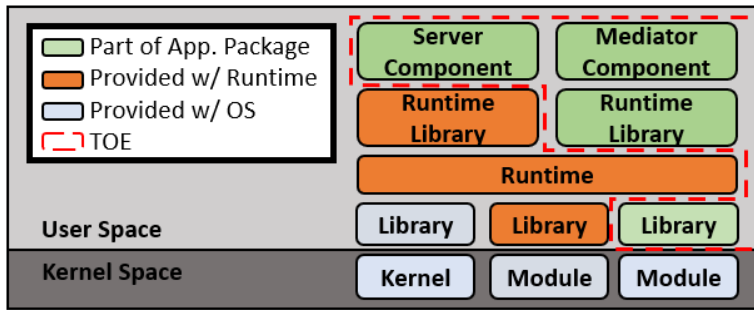
## 4.2  TOE Architecture

Software Requirements:

The TNMS Server is a pair of Java applications designed to run in the following operational environment:

- Red Hat Enterprise Linux (RHEL) 7.9 (64 bit) / CentOS 7.9 (64 bit) on a 64 bit Intel Xeon processor

- Amazon Corretto (OpenJDK) JDK/JRE 11.0.6

The TNMS Server TOE includes the following components that are co-located (and are depicted in Figure 1 below):

- Server component: The server component of the TNMS Server implements a TLS server that accepts TLS connections from a TNMS Client, operates on instructions sent from the TNMS Client and then uses mediator APIs as necessary to communicate with network entities to implement those instructions.

- Mediator component: The mediator component of the TNMS Server offers APIs used by the server component that enable it to securely communicate, using SSH (Java Secure Channel - JSch) as a client, with configured network entities via the mediator.

The TOE components communicate with each other through inter-process communication. The secure communication features all utilize Bouncy Castle (installed with the TNMS Server) for cryptographic operations.

*TOE Architecture*

## 4.3   Physical Boundaries

The TNMS Server TOE is a pair of Java applications (server and mediator) running on Amazon Corretto (OpenJDK) JDK/JRE version 11.0.6 operating in a RHEL / CentOS  7.9 (64 bit) environment.  The only external services the TOE depends on are a Certificate Authority for X509 certificate validation services, the TNMS Client with which the TNMS Server is configured to work, an Oracle database (that is installed on the same host platform and accessed locally), and network entities that are managed by the TNMS via secure communication from the mediator application.

# 5   Security Policy

This section summaries the security functionality of the TOE:
1. Cryptographic support
2. User data protection
3. Security management
4. Privacy
5. Protection of the TSF
6. Trusted path/channels

## 5.1   Cryptographic support

The TOE uses Automated Cryptographic Validation Test System (ACVTS)-validated cryptographic algorithm implementations, provided by the Bouncy Castle cryptographic module installed with the TOE, to support asymmetric key generation, encryption/decryption, signature generation and verification and establishment of trusted channels to protect data in transit. The TOE implements a TLS server to securely communicate with a TNMS Client, implements a SSH client to securely communicate with managed network entities, and implements functionality to securely store key data related to secure communications. The TOE also relies on the underlying Java platform to generate entropy that is used as input data for the TOE's deterministic random bit generator (DRBG).

## 5.2   User data protection

The TOE does not access any hardware resources or sensitive information repositories other than network access. No sensitive data outside of secure credentials is stored in non-volatile memory. Inbound and outbound network communications are restricted to those that are TOE-initiated to configured network elements, responding to incoming TNMS Clients TLS connections for remote management, and checking for updates.

## 5.3   Security management

After installation, an administrator manages the TOE through a TNMS client, and the TOE stores administrator configurations in its database stored in the platform file system.

When configured with default credentials or no credentials, the TOE restricts its functionality and only allows the ability to set new credentials.  By default, the TOE is configured with file permissions to protect itself and its data from unauthorized access.

## 5.4   Privacy

The TOE does not transmit personally identifiable information (PII) over any network interfaces.

## 5.5   Protection of the TSF

The TOE protects itself against exploitation by implementing address space layout randomization (ASLR) and by not allocating any memory region for both write and execute permission. The TOE uses standard platform APIs and includes a number of third party libraries used to perform its functions.

The TOE includes mechanisms to check for updates and to query the current version of the application software. TOE software is digitally signed and distributed using the platform-supported package manager. The TOE does not update its own binary code in any way and when removed, all traces of the TOE application software are deleted.

## 5.6   Trusted path/channels

The TOE protects communications between itself and managed network entities using SSH and between itself and the TNMS Client using TLS.

# 6  Documentation

The following documents were available with the TOE for evaluation:

- Infinera Transcend Network Management System Server 18.10.3 Administrative Guidance for Common Criteria, Version 1.1, December 6, 2022

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

# 7   Evaluated Configuration

The Target of Evaluation (TOE) is Transcend Network Management System (TNMS) Server version 18.10.3. The TNMS Server is a pair of Java applications designed to run in the following operational environment:

- Red Hat Enterprise Linux (RHEL) 7.9 (64 bit) / CentOS 7.9 (64 bit) on a 64-bit Intel Xeon processor

- Amazon Corretto (OpenJDK) JDK/JRE 11.0.6

# 8   IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report for Infinera Corporation Transcend Network Management System Server, Version 0.3, December 9, 2022 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

## 8.1   Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

## 8.2   Evaluation Team Independent Testing

The Evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the ASPP14/PKGTLS11/SSH10 including the tests associated with optional requirements. The AAR, in sections 1.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

# 9    Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding Evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 Rev 5. The evaluation determined the Transcend Network Management System Server TOE to be Part 2 extended, and to meet the SARs contained in the ASPP14/PKGTLS11/SSH10.

## 9.1   Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Infinera Transcend Network Management System Server 18.10.3 product that is consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validators reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

## 9.2   Evaluation of the Development (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally, the Evaluators performed the assurance activities specified in the ASPP14/PKGTLS11/SSH10 related to the examination of the information contained in the TSS.

The Validators reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

## 9.3   Evaluation of the Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validators reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

## 9.4   Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was identified.

The Validators reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the Evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

## 9.5   Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the ASPP14/PKGTLS11/SSH10 and recorded the results in a Test Report, summarized in the AAR.

The Validators reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

## 9.6   Vulnerability Assessment Activity (VAN)

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the Evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The Evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) on 12/01/2022 with the following search terms:

- Infinera
- Infinera Corporation
- Transcend Network Management System
- TNMS
- ASM
- AXL Software Radius
- Angular
- Animal Sniffer Annotations

- Apache ActiveMQ
- Apache Commons
- Apache Groovy
- Apache HttpClient
- Apache HttpComponents Core
- Apache Kafka
- Apache Log4j
- Apache Tomcat
- Apache XML

- Apache Xalan
- Apache Xerces2
- log4j
- AspectJ
- AsyncHttpClient
- AutoValue Annotations
- Avalon Framework
- Bouncy Castle TLS
- Batik
- Bootstrap (Twitter)

- Bouncy Castle
- CDIs
- Castor
- Checker Qual
- Common Annotations
- Dagger
- Db4o
- Disruptor
- Elsa Serialization
- Expression Language
- Extended StAX
- FindBugs jsr305
- GeoServer
- Goldman Sachs
- Gson
- Guice
- Guava
- H2 Database Engine
- Hamcrest
- HawtJNI Runtime
- Hibernate
- HyperSQL Database Engine
- Install Anywhere
- J2EE Connector Architecture
- J2EE Management
- J2ObjC Annotations
- JAVAX RMI
- JAXB Implementation
- JAXB Runtime
- JBoss EJB client
- JBoss Logging
- JBoss Marshalling
- JBoss Remoting
- JBoss classfilewriter
- JCL 1.2 Implemented Over SLF4J
- JDOM
- JFreeChart
- JFreeReport
- JFtp
- JGraphT

- JSON Web Token
- JSch
- JUL to SLF4J bridge
- JUnit
- JZlib
- JacORB
- Jackson
- Jakarta Annotations
- Jakarta JCS
- Jakarta XML
- Jansi
- Java Architecture for XML Binding
- Java Communications
- Java DMK
- Java Mail
- Java Servlet
- Java gRPC
- Java inject from the JSR-330 Expert Group
- Java Interceptors
- JavaBeans Activation
- JavaHelp
- JavaServer Pages TagLib Implementation
- Java Authentication and Authorization Service
- Javassist
- Jcommander
- Jetbrains
- Jline
- Jscape
- Koloboke Collections
- Kotlin Stdlib
- MapStruct
- Metrics Core
- Metrics Integration
- ModeShape
- Monfox TL1
- Netty Project
- OW2 Utilities

- OpenCensus
- OpenFusion CORBA Services
- Openmap
- Oracle Database JDBC Drivers
- Oracle Deinstallation
- Oracle Fast Infoset
- Oracle iStack
- Picocli
- Protocol Buffer Java
- Protocol Buffers
- Quartz
- Querydsl
- Reactor Components
- Remoting-jmx
- SLF4J
- SNMP4J
- SmoothieMap
- SnakeYAML
- Spring
- Spring Boot
- Spring Framework
- Spring Security
- Stax2
- Stormpot
- Super CSV
- TXW Runtime
- Thymeleaf
- Trove for Java
- Tyrex
- Undertow Core
- VT Crypt
- VT Dictionary
- VT Password
- Weld Core
- Wildfly
- Woodstox
- XML Commons External Components XML Extensions
- Xerces
- XmlSchema Core

- aosphere-cdi
- aosphere-runtime
- aosphere-socketio
- cglib
- codegen
- perfmark
- reflections
- JBoss Marshalling river
- spring-boot-actuator
- swingx
- syslog4j
- thymeleaf-extras-springsecurity4
- thymeleaf-layout-dialect
- thymeleaf-spring4
- ucp
- unbescape
- wasync

- webdavlib
- wildfly-common
- xenocom
- concurrent
- com.typesafe:config
- dom4j
- edtFTPj
- error-prone annotations
- exp4j
- fast-serialization
- google-gson
- image4j
- grpc-context
- istack commons
- jQuery
- jacorb
- javax.ejb
- javax.transaction
- jgraph

- jgraphx
- jmxremote_optional repackaged as module
- jmxtrans
- jt-classbreaks
- kotlin-argparser
- mysema-commons-lang
- level db
- logkit
- net.sourceforge.streamsupport:java9-concurrent-backport
- objenesis
- ognl
- ojdbc
- ojdbc8
- xnio-api.

The Validators reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

## 9.1   Summary of Evaluation Results

The Evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the Evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

# 10 **Validator Comments/Recommendations**

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Infinera Transcend Network Management System Server 18.10.3 Administrative Guidance for Common Criteria, Version 1.1, December 6, 2022. No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

# 11 **Annexes**

Not applicable

## 12 Security Target

The Security Target is identified as: Infinera Corporation Transcend Network Management System Server 18.10.3 Security Target, Version 1.5, December 9, 2022.

# 13 **Glossary**

The following definitions are used throughout this document:

| Term | Definition |
| --- | --- |
| Common Criteria Testing Laboratory (CCTL) | An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations. |
| Conformance | The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model. |
| Evaluation | The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated. |
| Evaluation Evidence | Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities. |
| Feature | Part of a product that is either included with the product or can be ordered separately. |
| Target of Evaluation (TOE) | A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC. |
| Validation | The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate. |
| Validation Body | A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme. |

**Table 2: Glossary**

# 14 **Bibliography**

The Validation Team used the following documents to produce this Validation Report:

[1]     Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

[2]     Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3]     Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4]     Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14).

[5]     Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11).

[6]     Functional Package for SSH, Version 1.0, 13 May 2021.

[7]     Infinera Corporation Transcend Network Management System Server 18.10.3 Security Target, Version 1.5, December 9, 2022 (ST).

[8]     Assurance Activity Report for Infinera Corporation Transcend Network Management System Server 18.10.3, Version 0.3, December 9, 2022 (AAR).

[9]     Detailed Test Report for Infinera Corporation Transcend Network Management System Server 18.10.3, Version 0.3, December 9, 2022 (DTR).

[10]    Evaluation Technical Report for Infinera Corporation Transcend Network Management System Server, Version 0.3, December 9, 2022 (ETR)

[11]    Infinera Transcend Network Management System Server 18.10.3 Administrative Guidance for Common Criteria, Version 1.1, December 6, 2022 (AGD).