National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report

for the

VMware ESXi 8.0 Update 3e

Report Number:	CCEVS-VR-VID11533-2025
Dated:	June 3, 2025
Version:	1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

Acknowledgements

Validation Team

Swapna Katikaneni

The Aerospace Corporation

Farid Ahmed

Michael Smeltzer

Russ Fink

John Hopkins University Applied Physics Lab

Common Criteria Testing Laboratory

Joachim Vandersmissen

Dick Sikkema

Hunter Barton

atsec information security corporation

Austin, TX

Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of VMware ESXi 8.0 Update 3e (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

This VR is intended to assist the end-user of this product and any security certification agent for that end- user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target ([ST]), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by atsec Common Criteria Testing Laboratory (CCTL) in Austin, TX, USA, and was completed in June 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by atsec. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Extended and meets the assurance requirements of the *Protection Profile, PP-Module* and *Functional Package* identified in Table 1.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activity Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, 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 ETR are consistent with the evidence produced.

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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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 IT 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 Product Compliant List (PCL).

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

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The *PP/PP-Module/Functional Package* to which the product is conformant
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	VMware ESXi 8.0 Update 3e
Security Target	VMware ESXi 8.0 Update 3e Security Target, Version 1.3, 2025-05-19
Sponsor & Developer	Broadcom, Inc.
Completion Date	June 2025
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	PP-Configuration for Virtualization and Server Virtualization Systems, Version 1.0, 4 June 2021, which contains the following: • Protection Profile for Virtualization, Version 1.1, 2021-06-14 • PP-Module for Server Virtualization Systems, Version 1.1, 2021-06-14 Functional Package for Transport Layer Security (TLS), Version 1.1, 2019-03-01
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 extended
CCTL	atsec information security corporation 4516 Seton Center Parkway Suite 250 Austin, TX 78759
Evaluation Personnel	Joachim Vandersmissen, Dick Sikkema, Hunter Barton
Validation Personnel	Swapna Katikaneni, Farid Ahmed, Michael Smeltzer, Russ Fink

3 TOE Architecture

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

The TOE is VMware ESXi 8.0 Update 3e, installed on a Dell PowerEdge R660 server with Intel Xeon Gold 6430 CPU. This CPU family was selected to provide the Intel VT and EPT feature support required by ESXi, as well as the RDSEED instruction used as an entropy source both internally and as a passthrough entropy source for virtual machines.

The TOE is VMware ESXi which is a Type 1 hypervisor that is installed onto a computer system with no host platform Operating System and serves as a virtual machine manager and virtualization system. This allows for the instantiation of multiple virtual machines onto a single physical platform. The TOE also implements mechanisms to enforce logical separation of VMs from one another and from the hypervisor so that data transmission between these domains can only occur through authorized interfaces. The TOE is a software-only TOE where the core component is installed directly on the bare metal hardware.

The TOE consists solely of the VMware ESXi 8.0 Update 3e hypervisor—the hardware platform on which it is evaluated provides the operational environment for the TOE. ***Figure 1*** shows the relationship between the TOE boundary and other components while ***Figure 2*** shows the external interfaces of the TOE.

Figure 1: TOE Boundary

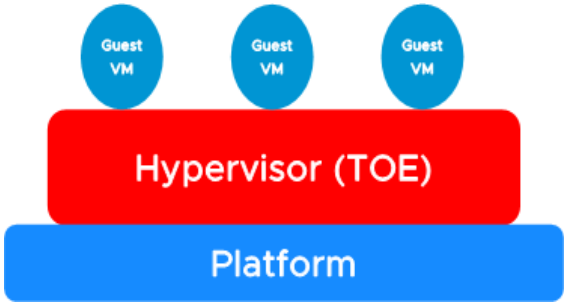
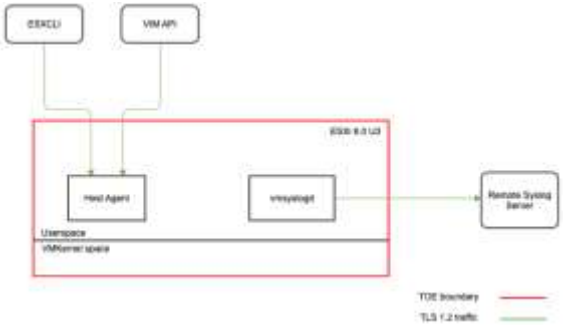


Figure 2: TOE External Interfaces



4 Environmental Strengths

The TOE provides the following security functions as described in the ST.

4.1 Security Audit

The TOE's security audit function accepts audit records and stores them locally in pre-allocated files, as well as transmitting them to a remote syslog server via TLS. Each audit record contains relevant information about the audit event. Locally stored audit records are reviewable by authorized subjects and protected from unauthorized deletion and modification.

4.2 Cryptographic Support

The TOE implements CAVP-validated cryptographic algorithms for its cryptographic services. These are used to support TLS and HTTPS communications. Trusted communications protocols are implemented using secure cryptographic parameters and in accordance with relevant standards. The TOE implements NIST SP 800-90A conformant Deterministic Random Bit Generator (DRBG) that is seeded with a hardware entropy source (Intel Xeon Gold 6430 CPU via RDSEED). The hardware entropy source used by the TOE is made available to Guest VMs through a passthrough interface.

4.3 User Data Protection

Authorized subjects may configure a specific Guest VM to use USB and network interfaces, however access to PCI passthrough devices, vGPU devices, and SCSI passthrough devices is always prohibited. All volatile and non-volatile memory is cleared prior to allocation to a Guest VM so that domain separation between Guest VMs is enforced.

4.4 Identification and Authentication

To control access to the TSF, the TOE uses locally defined username/password credentials for authentication. All TSF-mediated actions require successful authentication prior to authorization. The TSF protects against brute-force password authentication attempts by locking an offending user account for a period of time when an excessive number of failed attempts have been accumulated. The TSF also enforces configuration of password complexity policies to further reduce the chance that a brute force authentication attack will succeed.

The TOE uses X.509 certificate validation services for TLS server authentication. CRLs are used for revocation. The TSF rejects invalid certificates and those whose revocation status cannot be determined.

4.5 Security Management

The TOE includes management functions that allow for configuration of its own behavior as well as configuration and manipulation of Guest VMs, such as starting/stopping VMs, creating checkpoints for VMs, and configuring the VMs with virtual networking and physical device access. The TOE includes several management interfaces over which various management functions can be performed. The TOE implements role-based access control to grant members of different roles granular privileges to manage the TSF and its associated data.

4.6 Protection of the TSF

The TOE implements various mechanisms to protect itself from misuse. A Guest VM can only access devices assigned to it by an Administrator. Furthermore, the TOE validates parameters passed to virtual devices and implements controls for transferring removable media between Guest VMs. The TOE includes a hypercall interface that allows Guest VMs to interact with the hypervisor. The TOE also uses hardware assists to eliminate the need for shadow page tables and reduce the use of binary translation.

The TOE enforces isolation between Guest VMs and between VMs and itself. It also implements various protection methods in the execution environment to protect against memory-based attacks. TOE updates are also integrity protected using digital code signing verification.

4.7 TOE Access

The TOE supports the display of an advisory warning message regarding unauthorized use of the TOE before establishing an Administrator session.

4.8 Trusted Path/Channel

The TOE implements TLS and HTTPS for secure communications between itself and external entities, which include remote administrators and remote audit servers. The TOE also enforces unambiguous identification of Guest VMs to reduce the likelihood that a user will inadvertently input data to an unintended Guest VM.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the *PP, PP-Module,* and *Functional Package* to which it claims conformance for assumptions about the use of the TOE. Those assumptions are drawn from the claimed *PP, PP-Module,* and *Functional Package* as listed in Table 1.

5.2 Clarification of Scope

As with any evaluation, this evaluation shows only that the evaluated configuration meets the security claims made, with a certain level of assurance, achieved through performance by the evaluation team of the evaluation activities specified by the *PP*, *PP-Module*, and *Functional Package* referenced in Table 1.

- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in VMware ESXi 8.0 Update 3e Security Target ([ST]). Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- 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 TOE must be installed, configured, and managed as described in the documentation referenced in Section 6 of this VR.

6 Documentation

The vendor provides guidance documents describing the installation process for VMware ESXi 8.0 Update 3e, as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation is as follows:

- VMware ESXi 8.0 Update 3e NIAP Common Criteria Guidance Supplement, Version 1.3 2025-05-19 ([CCGUIDE])

To use the product in the evaluated configuration, configure it as specified in this document. Any additional documentation provided with the product, or that may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 IT Product Testing

This section describes the testing efforts of the evaluation team.

A non-proprietary description of the tests performed, and their results is provided in the Assurance Activity Report ([AAR]). A description of the test environment and a list of tools used for testing is provided in Section 2.3.4 of the AAR.

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the *PP*, *PP-Module*, and *Functional Package* listed in Table 1.

The evaluation team devised a Test Plan based on the Test Activities specified in the above *PP, PP-Module* and *Functional Package*. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

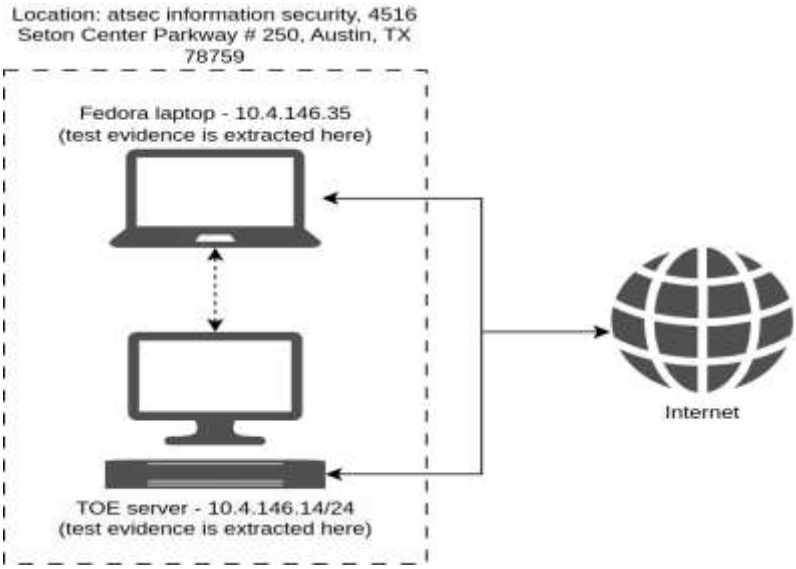
Independent testing took place at the atsec CCTL facility in Austin, TX, from December 2024 to May 2025.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements were fulfilled.

7.1 Test Configuration

The evaluation team established a test configuration comprising VMware ESXi 8.0 Update 3e running on Dell PowerEdge R660 server with Intel Xeon Gold 6430 CPU. The Dell PowerEdge R660 server was connected to a Lenovo ThinkPad T440p running the test tools as shown in the diagram below. Section 2.3.4 of the Assurance Activity Report ([AAR]) provides a detailed description of the test configuration the CCTL used to test the TOE.



8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The TOE comprises VMware ESXi 8.0 Update 3e, installed on a Dell PowerEdge R660 server with Intel Xeon Gold 6430 CPU.

Usage of other Intel CPUs is subject to equivalence arguments that are outside the scope of this evaluation.

8.2 Excluded Functionality

VMware ESXi additionally includes the following features that are not part of the evaluated TOE because they are outside the scope of the functionality described by the TOE's conformance claims:

- 3rd Party VIBs (distributed independently of VMware ESXi)
- Active Directory integration
- Common Information Model (CIM)
- Direct Console User Interface (DCUI)
- Internet Protocol Security (IPsec)
- NSX software
- PCI passthrough (i.e. VMDirectPath I/O), including vGPU
- Physical optical drives (CD/DVD)
- Raw disks (RDM passthrough of storage LUNs)

- Remote shell (SSH)
- SCSI passthrough
- Simple Network Management Protocol (SNMP)
- USB passthrough
- vCenter Server software
- Virtual Shared Disks (Multiwriter disks)
- VM encryption
- VM Virtual Disk sharing
- vMotion
- VMware PowerCLI software
- vSAN software.

Additionally, the Guest VM software is not provided by VMware. Customers supply their own operating systems from 3rd party operating system vendors (e.g., Microsoft Windows Server 2022). Guest VMs and their contents are outside the scope of the evaluation.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for VMware ESXi 8.0 Update 3e ([*ETR*]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

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, revision 5 ([CCPART1], [CCPART2], [CCPART3]) and CEM version 3.1, revision 5 ([CEM]), and the specific evaluation activities specified in the *PP*, *PP-Module*, and *Functional Package* listed in Table 1

The evaluation determined the TOE satisfies the conformance claims made in the VMware ESXi 8.0 Update 3e Security Target, of Part 2 extended and Part 3 extended. The TOE satisfies the requirements specified in the *PP*, *PP-Module*, and *Functional Package* listed in Table 1.

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

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS assurance activity and each work unit from ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, and ASE_TSS.1 CEM. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed *PP*, *PP-Module*, and *Functional Package*, and security function descriptions that satisfy the requirements.

9.2 Evaluation of the Development Activities (ADV)

The evaluation team performed each ADV assurance activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed *PP*, *PP-Module*, and *Functional Package* for design evidence. The ADV evidence consists of the TSS

descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

9.3 Evaluation of the Guidance Activities (AGD)

The evaluation team performed each AGD assurance activity and applied each AGD_OPE.1 and AGE_PRE.1 work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC assurance activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit to the extent possible given the evaluation evidence required by the claimed *PP*, *PP-Module*, and *Functional Package.* The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

9.5 Evaluation of the Test Documentation and the Test Activities (ATE)

The evaluation team performed each ATE assurance activity and applied each ATE_IND.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed *PP*, *PP-Module*, and *Functional Package* and recorded the results in the Test Report, summarized in the AAR.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA assurance activity and applied each AVA_VAN.1 CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed *PP*, *PP-Module*, and *Functional Package*. This comprised a search of public vulnerability databases.

The evaluator searched for publicly known vulnerabilities applicable to the VMware ESXi 8.0 Update 3e using the following sources:

- Broadcom security content disclosure statements for releases of VMware ESXi 8.0 Update 3 related to this evaluation:
  - https://support.broadcom.com/web/ecx/security-advisory then search for ESXi
- MITRE Common Vulnerabilities and Exposures (CVE) List:
  - https://cve.mitre.org/cve/search_cve_list.html
- National Vulnerability Database:
  - https://nvd.nist.gov/
- CISA Known Exploited Vulnerabilities Catalog:
  - https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- OpenSSL 3.0 Vulnerabilities:
  - https://openssl-library.org/news/vulnerabilities-3.0/index.html

Keywords used in CVE search:

- VMware ESXi
- ESXi 8.0 vmdk

- virtual machine disk
- virtual machine manager
- Dell PowerEdge
- Intel Xeon Gold 6430
- OpenSSL
- BoringSSL
- BoringCrypto
- Envoy
- VMKCrypto
- VMKernel Cryptographic Module

In addition to the lists of fixes published by the vendor, the evaluator performed manual searches throughout the evaluation process. The most recent search was performed on 2025-05-12 and the results of these searches did not identify any vulnerabilities that are applicable to the security functionality of the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the evaluation activities specified in the claimed *PP*. Furthermore, the evaluation team's testing demonstrates 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 configuration guide document listed in Section 6. No other versions of the TOE, either earlier or later, were evaluated. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated.

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. See Section 8.2 of this report for product functionality that is not included in the scope of evaluation. Additional functionality provided by entities in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness. All other items and scope issues have been sufficiently addressed elsewhere in this document.

11 Security Target

The ST for this product's evaluation is *VMware ESXi 8.0 Update 3e Security Target*, Version 1.3, 2025-05-19.

A Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
PCL	Product Compliant List
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VR	Validation Report

B Bibliography

The validation team used the following documents to produce this VR:

[CCPART1]	Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.
[CCPART2]	Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
[CCPART3]	Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017.
[CEM]	Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.
[PP_BASE_VIRTUALIZATION_V1.1]	Protection Profile for Virtualization, Version 1.1, 2021-06-14.
[MOD_SV_V1.1]	PP-Module for Server Virtualization Systems, Version 1.1, 2021-06-14.
[MOD_SV_V1.1-SD]	Supporting Document Mandatory Technical Document PP-Module for Server Virtualization Systems, Version 1.1, 2021-06-14
[PKG_TLS_V1.1]	Functional Package for Transport Layer Security (TLS), Version 1.1, 2019-03-01.
[ST]	VMware ESXi 8.0 Update 3e Security Target, Version 1.3, dated, 2025-05-19
[CCGUIDE]	VMware ESXi 8.0 Update 3e NIAP Common Criteria Guidance Supplement, Version 1.3, dated 2025-05-19.
[ETR]	Evaluation Technical Report VMware ESXi 8.0 Update 3e, Version 1.2, dated 2025-05-30
[AAR]	Assurance Activity Report VMware ESXi 8.0 Update 3e, Version 1.1, dated 2025-05-19