National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5

Report Number: CCEVS-VR-VID11525-2025
Dated: March 27, 2025
Version: 1.3

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

Jerome Myers, Ph.D.

Meredith M Martinez

The Aerospace Corporation

Common Criteria Testing Laboratory

Eugene Polulyakh

Diana Polulyakh

Valeriy Polulyakh, Ph.D.

Joseph R. Maixner

Advanced Data Security, LLC

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5. 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 Advanced Data Security, LLC (ADSec) Common Criteria Testing Laboratory (CCTL) in San Jose, CA, United States of America, and was completed in March 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Advanced Data Security, LLC. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the collaborative Protection Profile for Network Devices, Version 2.2e, 23-March-2020 (NDcPP2.2e).

The Target of Evaluation (TOE) is Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5.

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 Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5 Security Target, Version 1.4, March 26, 2025, 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 Product Compliant List.

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

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (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.

Table 1: Evaluation Identifiers

Name	Description
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5
Protection Profile	collaborative Protection Profile for Network Devices Version 2.2e, 23 March 2020
ST	Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5 Security Target, Version 1.4, March 26, 2025.
Evaluation Technical Report	Evaluation Technical Report for Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5, Version 1.3, March 26, 2025
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Pure Storage, Inc.
Developer	Pure Storage, Inc.
Common Criteria Testing Lab (CCTL)	Advanced Data Security, LLC
CCEVS Validators	Jerome Myers, Ph.D. and Meredith M. Martinez, *The Aerospace Corporation*

3. ARCHITECTURAL INFORMATION

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

Pure Storage, Inc.'s (Pure Storage) Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5 (TOE) is an enterprise Network Attached Storage solution that includes a Linux-based operating system, SAN (Storage Area Network) protocols and interfaces (iSCSI, Fiber Channel, SAS), and custom software to provide network storage with high performance, reliability, usability, and efficiency.

3.1 TOE EVALUATED PLATFORMS

The TOE consists of the following FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 hardware models:

FlashArray//X R4 & FlashArray//C R4 Family models and specifications

Model	X20 R4 / C20 R4	X50 R4 / C50 R4	X70 R4 / C70 R4	X90 R4 / C90 R4
CPU	Intel® Xeon® Silver 4410Y Processor	Intel® Xeon® Silver 4410Y Processor	Intel® Xeon® Gold 5416S Processor	Intel® Xeon® Gold 5418N Processor

Total Volatile Memory	256 GB	384 GB	512 GB	1024 GB
Management Ports	2 x 1Gb	2 x 1Gb	2 x 1Gb	2 x 1Gb
Local Console Ports	1x	1x	1x	1x

FlashArray//X R3 Family models and specifications

	X10 R3	**X20 R3**	**X50 R3**	**X70 R3**	**X90 R3**
CPU	Intel® Xeon® Silver 4208 Processor	Intel® Xeon® Silver 4210R Processor	Intel® Xeon® Silver 4214R Processor	Intel® Xeon® Gold 6230 Processor	Intel® Xeon® Silver 6252 Processor
Total Volatile Memory	96 GB	192 GB	288 GB	384 GB	768 GB
Management Ports	2 x 1Gb	2 x 1Gb	2 x 1Gb	2 x 1Gb	2 x 1Gb
Local Console Ports	1x	1x	1x	1x	1x

FlashArray//C R3 & FlashArray//XL Family models and specifications

	C60 R3	**C40 R3**	**XL130**	**XL170**
CPU	Intel Xeon Gold 6230 Processor	Intel Xeon Silver 4210R Processor	Intel® Xeon® Gold 6338 Processor	Intel® Xeon® Platinum 8368 Processor
Total Volatile Memory	768 TB	384 TB	768 GB	1 TB
Management Ports	2 x 1Gb	2 x 1Gb	2 x 1Gb	2 x 1Gb
Local Console Ports	1x	1x	1x	1x

Software: Each model of the TOE runs the Purity 6.5 Operating System software.

3.2 PHYSICAL BOUNDARIES

The TOE is Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5 including the following models: Flash Array X20 R3, Flash Array X50 R3, Flash Array X70 R3, Flash Array X90 R3, FlashArray X20 R4, FlashArray X50 R4, FlashArray X70 R4, FlashArray X90 R4, FlashArray C60 R3, FlashArray C40 R3, FlashArray C20 R4, FlashArray C50 R4, FlashArray C70 R4, FlashArray C90 R4, FlashArray XL130 and FlashArray XL170.

The TOE interfaces with the following non-TOE systems in its operational environment:

- Syslog server
- Network Time Protocol (NTP) Server

- Administrative Users

The scope of the evaluation was limited to the requirements in the ST – all other functionality was outside the scope of the evaluation.

4. SECURITY POLICY

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 SECURITY AUDIT

- The TOE generates and stores audit events locally and forwards the logs remotely to syslog server securely via TLS.
- The TOE will audit all events and information defined in Table 12: Auditable Events in the Security Target.
- The TOE will also include the identity of the user that caused the event (if applicable), date and time of the event, type of event, and the outcome of the event.
- The TOE protects storage of audit information from unauthorized deletion.
- The TOE prevents unauthorized modifications to the stored audit records.

4.2 CRYPTOGRAPHIC SUPPORT

The TSF performs the following cryptographic operations:

- SSH for remote CLI administrative management of the TOE:
  - Protocol versions:
    - SSHv2 (Conforming to RFCs 4251-4254, 4344, 5656, 6668, 8308 section3.1, 8332)
  - Public-Key Algorithms:
    - ssh-rsa2-256 - 2K-bit RSA key
    - ssh-rsa2-512 - 2K-bit RSA key
  - Data Encryption - Algorithms:
    - aes128-cbc - 128-bit AES symmetric key
    - aes256-cbc - 256-bit AES symmetric key
    - aes128-ctr - 128-bit AES symmetric key
    - aes256-ctr - 256-bit AES symmetric key
    - aes128-gcm@openssh.com - 128-bit AES symmetric key
    - aes256-gcm@openssh.com - 256-bit AES symmetric key
  - Data Encryption - MACs:
    - hmac-sha2-256, hmac-sha2-512
  - Key Exchange:
    - ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521
- Syslog Server:
  - Conforming to the following RFCs:
    - RFC 3164 - The BSD syslog Protocol, RFC 5425 - TLS Transport Mapping

    - Supporting the following for TLS:
        - TLSv1.2 (Conforming to RFC 5246)
    - Supporting at least one of the following TLS Ciphersuites:
        - TLS_RSA_WITH_AES_128_CBC_SHA
        - TLS_RSA_WITH_AES_256_CBC_SHA
        - TLS_RSA_WITH_AES_128_CBC_SHA256
        - TLS_RSA_WITH_AES_256_CBC_SHA256
- NTP Server:
    - Conforming to one of the following RFCs:
        - RFC 5905 - Network Time Protocol Version 4
    - Supporting one of the following NTP versions:
        - NTP v4
    - Supporting authentication using messages digests with the SHA-256 algorithm

The TSF zeroizes all plaintext secret and private cryptographic keys and CSPs once they are no longer required.

4.3 IDENTIFICATION AND AUTHENTICATION

The TSF supports passwords consisting of alphanumeric and special characters.

- The TSF allows the security administrator to configure the minimum password length from 1 character to 100 characters.
- The TSF prevents offending Administrator accounts from successfully establishing remote session using any authentication method that involves a password until an Administrator defined time period has elapsed
- The TSF allows local administrators to re-enable locked user accounts
- The TSF requires all administrative-users to authenticate before allowing the user to perform any actions other than:
    - Display the warning banner
    - Respond to ICMP Echo Request
    - Respond to ARP requests with ARP replies
    - Make DNS Requests

4.4 SECURITY MANAGEMENT

- TSF data includes the following:
    - All audit records generated to meet the auditing requirements of the PP
    - All user credentials (symmetric keys, private keys, keying material, username/password)
    - TSF Configuration data
- The TSF includes four administrative roles within the Authorized Administrator role:
    - Internal Administrator
    - Array Administrator
    - Storage Administrator
    - Read-Only Administrator
- All roles are considered authorized administrators.
- The device ships with three hard-coded users but allows for additional users to be created.
- The TOE provides management over SSH (remote) and a local console.
- The TOE authenticates administrative users using a username/password combination or a username/SSH_RSA key combination.
- The TSF does not allow access to any administrative functions prior to successful authentication.
- The TOE also has the capability of being updated and verifying updates via published hash verification.

4.5 PROTECTION OF THE TSF

- The TSF protects TSF data from disclosure when the data is transmitted between administrators and the TOE, and between the TOE and trusted IT entities.
- The TSF prevents the reading of secret and private keys.
- The TOE provides reliable time stamps for itself.
- The TOE runs a suite of self-tests during the initial start-up (upon power on) to demonstrate the correction operation of the TSF.

4.6 TOE ACCESS

- The TOE, for local interactive sessions, terminates the user's session after an Authorized Administrator-specified period of session inactivity (applies to the local console).
- The TOE terminates a remote interactive session after an Authorized Administrator-configurable period of session inactivity (applies to SSH remote console)
- The TOE allows Administrator-initiated termination of the Administrator's own interactive session.
- Before establishing an administrative user session, the TOE is capable of displaying an Authorized Administrator-specified advisory notice and consent warning message regarding unauthorized use of the TOE.

4.7 TRUSTED PATH/CHANNELS

The TOE supports TLSv1.2 to secure remote communications. TLS protocol may be used for communications with remote IT entities. Remote administration is only supported using SSH.

- The TOE uses TLS to provide a trusted communication channel between itself and all authorized IT entities that are logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.
- The TOE permits the TSF, or the authorized IT entities, to initiate communication via the trusted channel.
- The TOE permits remote administrators to initiate communication via the trusted path. The TOE provides an SSH protected trusted path to administer the TOE.
- The TOE requires the use of the trusted path for initial administrator authentication and all remote administration actions.

5. ASSUMPTIONS & CLARIFICATION OF SCOPE

5.1 ASSUMPTIONS

The Security Problem Definition, including the assumptions, may be found in the following document:

- collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 (NDcPP2.2e)

That information has not been reproduced here and the NDcPP2.2e 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 NDcPP2.2e 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.

5.2 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 collaborative Protection Profile for Network Devices 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 referenced in Section 6, additional customer documentation for the specific Network Device models was not included in the scope of the evaluation and therefore should not 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 NDcPP2.2e and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation, including:
    - Data reduction technology
    - Non-Disruptive Expansion and High Availability
    - Snapshots, Backup & Disaster Recovery including asynchronous replication, ActiveDR, ActiveCluster, and SafeMode
    - Data at rest encryption
    - Graphical User Interface
    - REST API
    - Remote Assist

6. DOCUMENTATION

The following documents were available with the TOE for evaluation:

- Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5 Guidance Document, version 4.5, March 2025

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 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. 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 (NDcPP2.2e) for Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5, Version 1.3, March 26, 2025 (DTR) as summarized in the Assurance Activity Report

(NDcPP2.2e) for Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5, Version 1.3, March 26, 2025 (AAR).

7.1 DEVELOPER TESTING

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

7.2 EVALUATION TEAM INDEPENDENT TESTING

The evaluation team verified the product according to the Common Criteria Certification document and ran the tests specified in the NDcPP2.2e including the tests associated with optional requirements. The specific test configurations and test tools utilized may be found in Section 5.5 of the AAR.

8. EVALUATED CONFIGURATION

The evaluated configuration is Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5. The Target of Evaluation (TOE) includes the following hardware models:

Model #	Processor	CPU Microarchitecture
Flash Array X10 R3	Intel Xeon Silver 4208	Cascade Lake
Flash Array X20 R3	Intel Xeon Silver 4210R	Cascade Lake
Flash Array X50 R3	Intel Xeon Silver 4214R	Cascade Lake
Flash Array X70 R3	Intel Xeon Gold 6230	Cascade Lake
Flash Array X90 R3	Intel Xeon Silver 6252	Cascade Lake
FlashArray X20 R4	Intel Xeon Silver 4410Y	Sapphire Rapids
FlashArray X50 R4	Intel Xeon Silver 4410Y	Sapphire Rapids
FlashArray X70 R4	Intel Xeon Gold 5416S	Sapphire Rapids
FlashArray X90 R4	Intel Xeon Gold 5418N	Sapphire Rapids
FlashArray C60 R3	Intel Xeon Gold 6230	Cascade Lake
FlashArray C40 R3	Intel Xeon Silver 4210R	Cascade Lake
FlashArray C20 R4	Intel Xeon Silver 4410Y	Sapphire Rapids
FlashArray C50 R4	Intel Xeon Silver 4410Y	Sapphire Rapids
FlashArray C70 R4	Intel Xeon Gold 5416S	Sapphire Rapids
FlashArray C90 R4	Intel Xeon Gold 5418N	Sapphire Rapids
FlashArray XL130	Intel Xeon Gold 6338	Ice Lake
FlashArray XL170	Intel Xeon Platinum 8368	Ice Lake

The models run the same firmware image.

To use the product in the evaluated configuration, the product must be configured as specified in the following documents.

- Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5. Guidance Document, version 4.5, March 2025.

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 Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP2.2e.

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 Pure Storage FlashArray Appliance products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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 evaluator performed the assurance activities specified in the NDcPP2.2e related to the examination of the information contained in the TSS.

The validator 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 validator 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 validator 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 NDcPP2.2e and recorded the results in a Test Report, summarized in the AAR.

The validator 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 performed a public search for vulnerabilities at the following sites and did not discover any residual vulnerabilities in the TOE. The evaluator searched the following sources for vulnerabilities:

- https://web.nvd.nist.gov/view/vuln/search
- http://cve.mitre.org/cve/
- https://www.cvedetails.com/vulnerability-search.php
- http://www.kb.cert.org/vuls/html/search
- www.exploitsearch.net
- www.securiteam.com
- http://nessus.org/plugins/index.php?view=search
- http://www.zerodayinitiative.com/advisories
- https://www.exploit-db.com/
- https://www.rapid7.com/db/vulnerabilities

The terms used for the search on 3/21/2025 were as follows:

- PureStorage
- FlashArray
- Pure Storage FlashArray X10 R3
- Pure Storage FlashArray X20 R3
- Pure Storage FlashArray X50 R3
- Pure Storage FlashArray X70 R3
- Pure Storage FlashArray X90 R3
- Pure Storage FlashArray X20 R4
- Pure Storage FlashArray X50 R4
- Pure Storage FlashArray X70 R4
- Pure Storage FlashArray X90 R4
- Pure Storage FlashArray C40 R3
- Pure Storage FlashArray C60 R3
- Pure Storage FlashArray C50 R4

- Pure Storage FlashArray C70 R4
- Pure Storage FlashArray C90 R4
- Pure Storage FlashArray XL130
- Pure Storage FlashArray XL170
- Intel Xeon Silver 4208
- Intel Xeon Silver 4210R
- Intel Xeon Silver 4214R
- Intel Xeon Gold 6252
- Intel Xeon Silver 4210R
- Intel Xeon Gold 6230
- Intel Xeon Silver 4410Y
- Intel Xeon Gold 5416S
- Intel Xeon Gold 5418N
- Intel Xeon Gold 6338
- Intel Xeon Platinum 8368
- Intel Xeon Silver 6252
- Purity//FA v6.5
- Purity 99.9.9
- Linux-base 4.5ubuntu9
- Bash 5.1-6ubuntu1
- Curl 7.81.0
- Libcurl 7.81.0
- Nginx 1.18.0
- Openjdk 8u382-ga-1~22.04.1
- Perl 5.34.0
- Tcpdump 4.99.1
- Sudo 1.9.9
- TLSv1.2
- OpenSSHv8.9p1
- OpenSSLv3.0.2

The validator 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.

9.7 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 Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5 Guidance Document, version 4.5, March 2025. 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. Other functionality provided by devices in the operational environment, such as the audit server, 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: *Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5. Security Target, Version 1.4, March 26, 2025*.

13. GLOSSARY

The following definitions are used throughout this document:

- **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.

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] collaborative Protection Profile for Network Devices, Version 2.2e, 23-March-2020 (CPP_ND_V2.2e),

[5] Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5. Security Target, Version 1.4, March 26, 2025. (ST)

[6] Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5. Guidance Document, Version 4.5, March 2025. (AGD)

[7] Assurance Activity Report (NDcPP2.2e) for Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5, Version 1.3, March 26, 2025 (AAR)

[8] Detailed Test Report (NDcPP2.2e) for Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5, Version 1.3, March 26, 2025 (DTR)

[9] Evaluation Technical Report for Pure Storage FlashArray//CR3, //CR4, //XL, //XR3, and //XR4 Appliances Running Purity 6.5, Version 1.3 March 26, 2025 (ETR)