National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report

Pure Storage Inc.

FlashArray//X running Purity//FA 5.3

Report Number: CCEVS-VR-11076-2021
Dated: January 13, 2021
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

Paul Bicknell
John Butterworth
Jenn Dotson
Patrick Mallett
Lisa Mitchell
Clare Olin
The MITRE Corporation

Anne Gugel
Peter Kruus
Johns Hopkins University Applied Physics Laboratory

Common Criteria Testing Laboratory

Devin Becker
Adam I. Borin
Gerrit Kruitbosch
UL, San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the assessment by the National Information Assurance Partnership (NIAP) Validation team of the evaluation of the FlashArray//X running Purity//FA 5.3 solution provided by Pure Storage, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by UL Verification Services Inc., a Common Criteria Testing Laboratory (CCTL) in San Luis Obispo, CA, United States of America, and was completed in January 2021. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by UL Verification Services, Inc. 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 2.1, 24 September 2018 (NDcPP21).

The TOE is the FlashArray//X running Purity//FA 5.3. The TOE identified in this Validation Report has been evaluated at a NIAP approved CCTL 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 (CCEVS) and the conclusions of the testing laboratory in the ETR 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 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the FlashArray//X running Purity//FA 5.3 Security Target, Version 3.2, January 7, 2021 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 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.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Target of Evaluation	FlashArray//X running Purity//FA 5.3
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.1
Security Target	FlashArray//X running Purity//FA 5.3 Security Target, version 3.2, January 7, 2021
Evaluation Technical Report	Common Criteria Evaluation Technical Report FlashArray//X running Purity//FA 5.3, Version 1.2, January 11, 2021 (20-4177-R-0015)
Common Criteria Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
Sponsor/Developer	Pure Storage, Inc.
Common Criteria Testing Lab	UL Verification Services Inc.
CCEVS Validators	Paul Bicknell, John Butterworth, Jenn Dotson, Anne Gugel,

	Peter Kruus, Patrick Mallett, Lisa Mitchell, Clare Olin

3 Architectural Information

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

Pure Storage Inc's (Pure Storage) FlashArray//X running Purity//FA 5.3 (the 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//X (R2 and R3 families) hardware models:

FlashArray//X R2 Family models and specifications:

	X10 R2	**X20 R2**	**X50 R2**	**X70 R2**	**X90 R2**
CPU	Intel® Xeon® Silver 4108 Processor	Intel® Xeon® Silver 4114 Processor	Intel® Xeon® Silver 4116 Processor	Intel® Xeon® Gold 6130 Processor	Intel® Xeon® Gold 6152 Processor
Total Volatile Memory	96GB	192GB	192GB	384GB	768GB
Management Ports	2 x 1Gb Management Ports 1x Local Console Port	2 x 1Gb Management Ports 1x Local Console Port	2 x 1Gb Management Ports 1x Local Console Port	2 x 1Gb Management Ports 1x Local Console Port	2 x 1Gb Management Ports 1x Local Console Port

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® Silver 6230 Processor	Intel® Xeon® Silver 6252 Processor
Total Volatile Memory	96GB	192GB	288GB	384GB	768GB
Management Ports	2 x 1Gb Management Ports 1x Local Console Port	2 x 1Gb Management Ports 1x Local Console Port	2 x 1Gb Management Ports 1x Local Console Port	2 x 1Gb Management Ports 1x Local Console Port	2 x 1Gb Management Ports 1x Local Console Port

Software:
Each model of the TOE runs the Purity//FA 5.3 Operating System software.

3.2 Physical Boundaries

Each TOE model is made up of FlashArray//X hardware with Purity//FA 5.3 software components. The TOE communicates with a remote syslog server and may be administered via a web browser or SSH client in the environment or the local console. Evaluated protocols and ciphersuites are detailed in the ST. 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 contains the security functions within the logical boundaries of the TOE. The following Security Functions are supported by the TOE:

- Audit
- Cryptographic Operations
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

4.1 Audit

- The TOE will audit all events and information defined in Table 3: 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.
- The TOE can transmit audit data to an external IT entity using the Syslog over TLS protocol.

4.2 Cryptographic Operations

The TSF performs the following cryptographic operations:

- SSH for remote CLI administrative management of the TOE:
    - Protocol versions: SSHv2 (Conforming to RFCs 4251-4254, 5656, and 6668)
    - Public-Key Algorithms: SSH-RSA, 2048-bit RSA keys
    - Data Encryption:
        - AES-CBC-128, 128-bit, AES symmetric key
        - AES-CBC-256, 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 Integrity: hmac-sha1, hmac-sha2-256, hmac-sha2-512, "Implicit"
    - Key Exchange: diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384,
      ecdh-sha2-nistp521
- HTTPS for remote administrative management of the TOE:
    - Protocol versions supporting: HTTPS/TLSv1.2 (Conforming to RFCs 2818 & 5246)
    - Supporting the following TLS Ciphersuites:
        - TLS_RSA_WITH_AES_128_CBC_SHA
        - TLS_RSA_WITH_AES_256_CBC_SHA
        - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
        - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
        - TLS_RSA_WITH_AES_128_CBC_SHA256
        - TLS_RSA_WITH_AES_256_CBC_SHA256
        - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
        - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
        - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
        - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
        - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

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 (FIA_AFL.1.1) 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 user accounts locked by the FIA_AFL.1 functionality.
- The TSF requires all administrative users to authenticate before allowing the user to perform any actions other than:
    - Display the warning banner in accordance with FTA_TAB.1;
    - Respond to ICMP Echo Request;

  - Respond to ARP requests with ARP replies;
  - Make DNS Requests;
  - Respond to HTTP Get Requests on TCP port 80 with a HTTP 301 'Moved Permanently' Status; Code redirecting to TCP port 443; and
  - Respond to TLS Client_Hello messages with TLS Server_Hello messages on TCP port 443.

4.4 Security Management

- TSF data includes the following:
  - All audit records generated to meet the auditing requirements of the Protection Profile;
  - All user credentials (symmetric keys, private keys, keying material, username/password); and
  - TSF Configuration data.
- The TSF includes four administrative roles within the Authorized Administrator role:
  - Internal Administrator,
  - Array Administrator,
  - Storage Administrator; and
  - Read-Only Administrator.
- All roles are considered authorized administrators for the remainder of this document.
- The device ships with three hard-coded users but allows for additional users to be created.
- The TOE provides management over HTTPS (remote), 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.
- The TOE provides a means to verify firmware/software updates to the TOE using a published hash mechanism to verify the candidate update package prior to installing the update.

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 and HTTPS remote web GUI console).
- The TOE allows Administrator-initiated termination of the Administrator's own interactive session.
- Before establishing an administrative user session, the TOE can display an Authorized Administrator-specified advisory notice and consent warning message regarding unauthorized use of the TOE.

4.7 Trusted Path/Channels

- The TOE uses TLS to provide a trusted communication channel between itself and all authorized IT entities that is 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 HTTPS protected trusted path, as well as 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

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

- collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018

That information has not been reproduced here and the NDcPP21 should be consulted if there is interest in that material.

This evaluation was limited to the functionality and assurances covered in the NDcPP21 as described for this TOE in the ST. 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.

6 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 in accordance with the assurance activities specified in the NDcPP21 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.
- 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 NDcPP21 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7 Documentation

The following guidance documents are provided in PDF format via download from the Pure Storage support web portal. Only the documents in **bold** were utilized for meeting the CC guidance requirements and only they should be trusted for the purpose of installing, administering, or using the product in its evaluated configuration. Any other documents should not be trusted for those purposes.

Document	Revision	Date
Guidance Documentation Pure Storage FlashArray//XR2 and //XR3 Appliances Running Purity 5.3	4.2.5	January 2021
FlashArray User Guide	5.3.0	August 22, 2019

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 Assurance Activity Report FlashArray//X running Purity//FA 5.3, V1.2, January 11, 2021 (AAR) and the FlashArray//X running Purity 5.3 Test Report, V1.4, 1/7/21 (DTR). The DTR shows the test configuration, provides the tested platforms, and lists the test tools.

8.1 Developer Testing

No evidence of Developer testing was provided or required.

8.2 Evaluation Team Independent Testing

The Evaluation team performed the independent testing activities to confirm the TOE operates to the TOE security functional requirements as specified in the ST for a product claiming conformance to the collaborative Protection Profile for Network Devices Version 2.1, September 24, 2018. The Evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the Supporting Document for the NDcPP21. The Test Plan described how each test activity was to be performed. The evaluation team executed the tests specified in the Test Plan and documented the results in a proprietary DTR noted in Section 8. The results of the testing are summarized in the publicly available AAR for this evaluation.

The hardware/software was provided in the same form that customers of the vendor would receive the product in. The evaluator installed and configured the TOE in accordance with the vendor provided guidance documentation and performed the testing procedures as described in the DTR.

9 Evaluated Configuration

The evaluated configuration consists of the models as defined in Section 3.1 of this Validation Report.

Configuration was performed in accordance with the documentation provided in Section 7. Instructions include configuration of remote syslog destination and transmission parameters. NTP functionality is unevaluated and Security Administrative users are instructed to disable NTP functionality in the evaluated configuration.

10 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.

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

10.1 Evaluation of the Security Target (ASE)

The Evaluation team applied each ASE CEM work unit and ensured the ST contained a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by FlashArray//X running Purity//FA 5.3 that are 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.

10.2 Evaluation of the Development (ADV)

The Evaluation team applied each ADV CEM work unit, 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 ST and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the NDcPP21 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.

10.3 Evaluation of the Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit and 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.

10.4 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.

10.5 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 NDcPP21 and recorded the results in the DTR, 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.

10.6 Vulnerability Assessment Activity (VAN)

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is provided in the AAR and ETR 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 vulnerability research is current as of January 6, 2021.

The search for publicly known vulnerabilities was performed against the sources and on the search-terms required in the NDcPP21 Supporting Document as well as the terms derived from the information that was available to the evaluators (vendor documentation, information gleaned from working with the products CLI, and information gleaned from automated packet analysis). In addition to the search terms required as per the Supporting Document, the following search terms were utilized: flash array, OpenSSH, OpenSSL, Pure Storage Flash Array //X R2 and //X R3, purestorage, pure storage, flasharray, purity, X R2, X R3, Lldpd, Nginx, Net-snmp, Syslog-ng, and Ubuntu.

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.

10.7 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.

11 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 documentation referenced in Section 7 of this Validation Report. No versions of the TOE and software, either earlier or later were evaluated.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, should be assessed separately and no further conclusions can be drawn about their effectiveness.

As noted earlier in this report, NTP functionality is unevaluated; Security Administrators are instructed to disable NTP functionality in the evaluated configuration.

12 Security Target

The Security Target is identified as: FlashArray//X running Purity//FA 5.3 Security Target, Version 3.2, January 7, 2021.

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.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, Version 3.1 Revision 5, CCMB-2017-04-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, April 2017, Version 3.1 Revision 5, CCMB-2017-04-004.

[5] collaborative Protection Profile for Network Devices Version 2.1, September 24, 2018

[6] FlashArray//X running Purity//FA 5.3 Security Target, Version 3.2, January 7, 2021

[7] Assurance Activity Report FlashArray//X running Purity//FA 5.3, V1.2, January 11, 2021

[8] Common Criteria Evaluation Technical Report FlashArray//X running Purity//FA 5.3, Version 1.2, January 11, 2021

[9] FlashArray//X running Purity 5.3 Test Report, V1.4, 1/7/21