

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



Validation Report

for

NetApp Storage Encryption (NSE) Running ONTAP 9.14.1

Report Number: CCEVS-VR-VID11477-2024
Dated: November 18, 2024
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

Lisa Mitchell

Lori Sarem

Randy Heimann

Chris Thorpe

The MITRE Corporation

Common Criteria Testing Laboratory

*Leidos Inc.
Columbia, MD*

Table of Contents

1	Executive Summary	1
2	Identification	2
3	TOE Architecture	4
4	Security Policy	6
4.1	Cryptographic Support	6
4.2	Security Management	6
4.3	Protection of the TSF	6
5	Assumptions and Clarification of Scope.....	7
5.1	Assumptions	7
5.2	Clarification of Scope	8
5.3	Excluded Functionality.....	8
6	Documentation	10
7	IT Product Testing	11
7.1	Test Configuration	11
8	Evaluated Configuration	13
9	Results of the Evaluation	14
9.1	Evaluation of the Security Target (ST) (ASE).....	14
9.2	Evaluation of the Development (ADV)	14
9.3	Evaluation of the Guidance Documents (AGD)	14
9.4	Evaluation of the Life Cycle Support Activities (ALC)	14
9.5	Evaluation of the Test Documentation and the Test Activity (ATE)	15
9.6	Vulnerability Assessment Activity (AVA)	15
9.7	Summary of Evaluation Results	16
10	Validator Comments/Recommendations	17
11	Security Target	18
12	Abbreviations and Acronyms	19
13	Bibliography	20

List of Tables

Table 1: Evaluation Identifiers	2
---------------------------------	---

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of NetApp Storage Encryption (NSE) running ONTAP 9.14.1 (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 Validation Report (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 Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed on November 8, 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Leidos. The evaluation determined that the TOE is:

- Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant

and demonstrates exact conformance to:

- *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0* + Errata 20190201, February 1, 2019 [5]

as clarified by all applicable Technical Decisions.

The TOE is NetApp Storage Encryption (NSE) running ONTAP 9.14.1.

The TOE identified in this VR 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). 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 documented in the Evaluation Technical Report (ETR) and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). The conclusions of the testing laboratory in the Evaluation Technical Report are consistent with the evidence produced. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the ST [7].

2 Identification

The Common Criteria Evaluation and Validation Scheme (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 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 who desire 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-Modules 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	NetApp Storage Encryption (NSE) Running ONTAP 9.14.1
Security Target	NetApp Storage Encryption (NSE) Running ONTAP 9.14.1 Security Target, Version 1.7, November 7, 2024
Sponsor & Developer	NetApp, Inc 3060 Olsen Drive San Jose, CA 95128
Completion Date	November 8, 2024
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	<i>collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition</i> , Version 2.0 + Errata 20190201, February 1, 2019
Conformance Result	PP Compliant, CC Part 2 Extended, CC Part 3 Conformant
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046

Item	Identifier
Evaluation Personnel	Anthony Apted Greg Beaver Pascal Patin
Validation Personnel	Lisa Mitchell Lori Sarem Randy Heimann Chris Thorpe

3 TOE Architecture

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

NetApp Storage Encryption (NSE) running ONTAP 9.14.1 (the TOE) is an authorization acquisition product that obtains and maintains authorization data used to access encrypted data stored on a full disk encryption product. It provides authorization data to third party self-encrypting drives (SEDs).

The TOE is provided pre-installed on NetApp disk storage appliances consisting of storage controllers and one or more enclosures of third-party SEDs. The TOE supports SEDs that follow either the Trusted Computing Group's (TCG) Opal or Enterprise standards. Both standards support the use of an Authentication Key (AK) and one or more Data Encryption Keys (DEK) per drive. ONTAP, the TOE's operating system, uses the AK to unlock a SED. Once the SED verifies that the AK is correct, it uses the AK to decrypt the drive's DEK(s).

The TOE in its evaluated configuration requires the use of its Onboard Key Manager (OKM) to manage the AK used to unlock the array's SEDs. Furthermore, the OKM must be configured with CC mode enabled. When CC mode is enabled, the OKM requires entry of a Cluster Passphrase every time the storage array is booted.

The Cluster Passphrase is an administrator-generated ASCII string, from 64 to 256 characters long, that is used as the authorization factor. The Cluster Passphrase is used in conjunction with a salt value (the Cluster Salt) to derive the Cluster Passphrase Key Encryption Key (CP-KEK), via an approved password-based key derivation function (PBKDFv2, as specified in NIST SP 800-132). The CP-KEK is then used to unwrap the Cluster Key Encryption Key (CKEK) and the CKEK is used to unwrap the AK, which in TOE terms is the Border Encryption Value (BEV). The Cluster Salt, CKEK, and AK, are all generated by the TOE's deterministic random bit generator (DRBG). The TOE uses key wrapping as defined in NIST SP 800-38F to protect the AK (wrapped using the CKEK) and the CKEK (wrapped using the CP-KEK) when storing the AK and CKEK in non-volatile memory.

Customers use storage virtual machines (SVMs) to serve data to clients and hosts. An SVM is a logical entity that abstracts physical resources. Data accessed through the SVM is not bound to a location in storage. Network access to the SVM is not bound to a physical port.

In addition to data volumes, ONTAP also uses the following special volumes (note: these volumes, like all volumes on an NSE system, are hosted on third party self-encrypting drives):

- A node root volume (typically "vol0") contains node configuration information and logs
- An SVM root volume serves as the entry point to the namespace provided by the SVM and contains namespace directory information
- System volumes contain special metadata such as service audit logs.

ONTAP prevents customers from storing user data on these special volumes.

In addition to data SVMs, ONTAP deploys special SVMs for administration:

- An admin SVM is created when the cluster is set up
- A node SVM is created when a node joins a new or existing cluster
- A system SVM is automatically created for cluster-level communications in an IP space.

The administrative SVMs listed above cannot be used to serve data. All administration is performed via the CLI accessed using a console directly connected to the appliance's RS-232 port.

In the evaluated configuration, the NetApp Volume Encryption must be configured and managed via the appliance's RS-232 console port. NetApp Storage Encryption also supports various networking protocols including SSH, CIFS, NFS, HTTP, HTTPS, DHCP, SNMP, Fibre Channel, and iSCSI, among others. The Protection Profile ([CPP_FDE_AA_V2.0E]) associated with this product did not include networking protocols as part of the security functional requirements and, as a result, does not include any requirements for assessing those protocols. Consequently, the protocols have not been examined as part of the required assurance activities and, therefore, no claims are made about the TOEs networking protocols.

The vendor recommends customers of the TOE consider the impact of using the product's SSH or HTTPS interfaces to manage the product, as opposed to the product's RS-232 console interface. Customers should base their decision on the environment in which the TOE operates and the value of the data that needs to be protected.

4 Security Policy

The TOE enforces the following security policies as described in the ST.

4.1 Cryptographic Support

The TOE includes NIST CAVP-validated cryptographic algorithms supporting cryptographic functions. The TOE provides key wrapping, key derivation, and validation of the Border Encryption Value (BEV).

4.2 Security Management

The TOE supports management functions for forwarding requests to change the Data Encryption Key (DEK) to the Encryption Engine (EE), forwarding requests to cryptographically erase the DEK to the EE, allowing authorized users to change authorization factors or set of authorization factors used, and initiate TOE software updates using a command line interface.

4.3 Protection of the TSF

The TOE provides trusted firmware updates, protects keys and key material, and supports Compliant power saving states. The TOE runs a suite of self-tests during initial start-up (on power on).

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the PP to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows:

- Users enable Full Drive Encryption on a newly provisioned or initialized storage device free of protected data in areas not targeted for encryption. The cPP does not intend to include requirements to find all the areas on storage devices that potentially contain protected data. In some cases, it may not be possible – for example, data contained in “bad” sectors. While inadvertent exposure to data contained in bad sectors or un-partitioned space is unlikely, one may use forensics tools to recover data from such areas of the storage device. Consequently, the cPP assumes bad sectors, un-partitioned space, and areas that must contain unencrypted code (e.g., MBR and AA/EE pre-authentication software) contain no protected data.
- Upon the completion of proper provisioning, the drive is only assumed secure when in a powered off state up until it is powered on and receives initial authorization.
- Communication among and between product components (e.g., AA and EE) is sufficiently protected to prevent information disclosure. In cases in which a single product fulfils both cPPs, then the communication between the components does not extend beyond the boundary of the TOE (e.g., communication path is within the TOE boundary). In cases in which independent products satisfy the requirements of the AA and EE, the physically close proximity of the two products during their operation means that the threat agent has very little opportunity to interpose itself in the channel between the two without the user noticing and taking appropriate actions.
- Authorized users follow all provided user guidance, including keeping password/passphrases and external tokens securely stored separately from the storage device and/or platform.
- The platform in which the storage device resides (or an external storage device is connected) is free of malware that could interfere with the correct operation of the product.
- External tokens that contain authorization factors are used for no other purpose than to store the external token authorization factors.
- The user does not leave the platform and/or storage device unattended until all volatile memory is cleared after a power-off, so memory remnant attacks are infeasible. Authorized users do not leave the platform and/or storage device in a mode where sensitive information persists in non-volatile storage (e.g., lock screen). Users power the platform and/or storage device down or place it into a power managed state, such as a “hibernation mode”.
- Authorized administrators ensure password/passphrase authorization factors have sufficient strength and entropy to reflect the sensitivity of the data being protected.
- The product does not interfere with or change the normal platform identification and authentication functionality such as the operating system login. It may provide authorization factors to the operating system's login interface, but it will not change or degrade the functionality of the actual interface.
- All cryptography implemented in the Operational Environment and used by the product meets the requirements listed in the cPP. This includes generation of external token authorization factors by a RBG.

- The platform is assumed to be physically protected in its Operational Environment and not subject to physical attacks that compromise the security and/or interfere with the platform's correct operation.

5.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. 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 evaluation activities specified in *Supporting Document – Mandatory Technical Document – Full Drive Encryption: Authorization Acquisition*, Version 2.0 + Errata 20190201, 1 February 2019 [6] and performed by the evaluation team).
- This evaluation covers only the specific software distributions and versions 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 NetApp Storage Encryption (NSE) running ONTAP 9.14.1 Security Target, Version 1.6, September 25, 2024 [7].
- 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 Validation Report.
- The TOE supports various networking protocols, including SSH, CIFS, NFS, HTTP, HTTPS, DHCP, SNMP, Fibre Channel, and iSCSI, among others. The *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition* does not consider and does not include networking protocols as part of the security functional requirements and, consequently, did not include any requirements for assessing those protocols. As a result, the protocols have not been examined as part of the required assurance activities and, therefore, no claims are made about the TOEs networking protocols.
- Configuration and administration of the TOE was bound to the RS-232 console interface. The use of HTTPS and/or SSH to manage the TOE is outside the scope of the evaluated configuration.

5.3 Excluded Functionality

The list below identifies features or protocols that are not evaluated or must be disabled, and the rationale why. Note that this does not mean the features cannot be used in the evaluated configuration (unless explicitly stated so). It means that the features were not evaluated and/or validated by an independent third party and the functional correctness of the implementation is vendor assertion. Evaluated functionality is scoped exclusively to the security functional requirements specified in the Security Target.

Feature	Description
SnapLock	<p>NetApp SnapLock is the WORM (write once, read many) compliance replication solution from NetApp. It provides integrated data protection for workloads that need to adhere to regulatory guidelines such as HIPAA, SEC 17a-4(f) rule, FINRA, and CFTC as well as national requirements for German-speaking countries (DACH).</p> <p>SnapLock was not included in the evaluation and was not tested in the evaluated configuration.</p>
Trusted Platform Module (TPM)	<p>The encryption keys for the onboard key manager (OKM) are not sealed by a physical TPM when running in Common Criteria mode.</p>
MetroCluster	<p>NetApp MetroCluster (MC) software is a solution that combines array-based clustering with synchronous replication to deliver continuous availability and zero data loss at the lowest cost.</p> <p>MetroCluster was not included in the evaluation and was not tested in the evaluated configuration.</p>
System Manager GUI	<p>The System Manager GUI is considered out of scope and all management is performed via the command line interface.</p>
VMware Virtualization	<p>VMware Virtualization was not included in the evaluation and was not tested in the evaluated configuration.</p>
Cloud environments	<p>ONTAP instances running within a cloud environment were not included in the evaluation and were not tested in the evaluated configuration.</p>

6 Documentation

NetApp offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The following documents, part of the ONTAP 9.14.1 documentation set, are included in the TOE documentation and were examined during the evaluation:

- NetApp Storage Encryption: Common Criteria Configuration Guide Version 1.4, November 7, 2024 [8]
- NetApp ONTAP 9.14.1 commands, June 26, 2024 [9]
- NetApp Set up, upgrade and revert ONTAP- ONTAP 9, July 02, 2024 [10]

To use the product in the evaluated configuration, the product must be configured as specified in these guides. 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. It is derived from information contained in the following proprietary document:

- *NetApp Storage Encryption (NSE) running ONTAP 9.14.1 Common Criteria Test Report and Procedures, Version 1.1, 7 November 2024* [13]

A non-proprietary description of the tests performed and their results is provided in the following document:

- *Assurance Activities Report For NetApp Storage Encryption (NSE) running ONTAP 9.14.1, Version 1.1, November 8, 2024* [11]

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 *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition* ([5]).

The evaluation team devised a Test Plan based on the Test Activities specified in *Supporting Document – Mandatory Technical Document – Full Drive Encryption: Authorization Acquisition*. 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 from June to October 2024. All testing artifacts were collected during on-site testing at Netapp’s facility in Raleigh, North Carolina, from June 24 to June 26, 2024. Due to the requirement to use the vendor’s proprietary coretool program to decompress core dumps the analysis of those dumps only took place after artifact collection was complete.

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 for *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition* were fulfilled.

7.1 Test Configuration

The evaluation team established a test configuration comprising:

- TOE components:
 - ONTAP 9.14.1 installed on following NetApp Storage Encryption appliances:
 - A150
 - A320
 - A400
 - FAS9500
- Test environment components:
 - Kali Linux Server (Release 2024.1), used as a storage client (i.e., client to access the storage arrays and disk volumes managed on the NetApp appliances under test)
 - Microsoft Windows 10 Enterprise workstation, supporting the following testing tools:

- WinHex 19.9
- HxD 2.4.

8 Evaluated Configuration

The TOE is NetApp Storage Encryption (NSE) running ONTAP 9.14.1. The physical boundary of the TOE is the binary files comprising the ONTAP 9.14.1 software.

The non-TOE hardware required by and provisioned with the TOE is identified in the table below.

NetApp Controllers Covered by the Evaluation

NetApp Controllers	Disk Type	Controller Form Factor
AFF A150	SSD	2U/24 internal drives
AFF A220	SSD	2U/24 internal drives
AFF A250	NVMe/SSD	2U/24 internal drives
AFF A300	SSD	3U
AFF A320	NVMe	2U
AFF A400	NVMe/SSD	4U
AFF A800	NVMe/SSD	4U/48 internal drives
AFF A900	NVMe/SSD	8U
AFF C190	SSD	2U/24 internal drives
AFF C250	NVMe	2U/24 internal drives
AFF C400	NVMe	4U
AFF C800	NVMe	4U
ASA A150	SSD	2U/24 internal drives
ASA A250	NVMe	2U/24 internal drives
ASA A400	NVMe/SSD	4U
ASA A800	NVMe/SSD	4U/48 internal drives
ASA A900	NVMe/SSD	8U
ASA C250	NVMe	2U/24 internal drives
ASA C400	NVMe	4U
ASA C800	NVMe	4U
ASA AFF A220	SSD	2U/24 internal drives
FAS2720	HDD/SSD	2U/12 internal drives
FAS2750	HDD/SSD	2U/24 internal drives
FAS2820	HDD/SSD	2U/12 internal drives
FAS500f	NVMe	2U/24 internal drives
FAS8200	HDD/SSD	3U
FAS8300	HDD/SSD	4U
FAS8700	HDD/SSD	4U
FAS9500	HDD/SSD	8U

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 NetApp Storage Encryption (NSE) Running ONTAP 9.14.1 (Proprietary) [12]. 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 ([1], [2], [3]) and CEM version 3.1, revision 5 ([4]), and the specific evaluation activities specified in *Supporting Document – Mandatory Technical Document – Full Drive Encryption: Authorization Acquisition, Version 2.0 + Errata 20190201, 1 February 2019* ([6]). The evaluation determined the TOE satisfies the conformance claims made in the NetApp Storage Encryption (NSE) running ONTAP 9.14.1 Security Target, of Part 2 Extended and Part 3 Conformant. The TOE satisfies the requirements specified in *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, 1 February 2019* ([5]).

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

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

The evaluation team performed each TSS assurance activity and ASE CEM work unit. 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 Protection Profile, and security function descriptions that satisfy the requirements.

9.2 Evaluation of the Development (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 Protection Profile 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 Documents (AGD)

The evaluation team performed each guidance assurance activity and applied each AGD 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 Protection Profiles. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence.

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

The evaluation team performed each test activity and applied each ATE_FUN.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP 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. The vulnerability analysis comprised a public domain search for potential vulnerabilities.

The evaluator performed searches of the specified public vulnerability databases on 22 July 2024, 9 September 2024, and 24 September 2024, and November 8, 2024.

The evaluation team searched the following public vulnerability repositories.

- Common Vulnerabilities and Exposures: https://cve.mitre.org/cve/search_cve_list.html
- National Vulnerability Database: <https://nvd.nist.gov/>
- US-CERT: <http://www.kb.cert.org/vuls/html/search>.
- OpenSSL: <https://www.openssl.org/news/fips-cve.html>

The evaluation team used the following search terms in the searches of these repositories:

- Product name—the evaluation team searched on the following terms:
 - “netapp”/ “netapp ontap”
 - “ontap”
 - “netapp fas”
 - “netapp aff”
 - “network storage encryption”
- Underlying components—the evaluation team searched on the following terms:
 - “ontap 9.14.1”
 - “OpenSSL 3.0.8 FIPS
 - “Intel ISA-L_crypto v 2.2”
 - “intel storage acceleration library”
 - Solid State drives (SSD) used with the TOE
 - AFF A150: KPM6WRUG960G (960GB SAS SSD)
 - AFF A320: MZWLJ3T8HBL5-000G6 (3.8TB NVMe)
 - AFF A400: XS960SE70104 (960GB SAS SSD)
 - Hard Disk Drive (HDD) used with the TOE
 - FAS9500: WUS721010AL5205 (10TB SAS HDD)
 - Third Party Hardware Components available for use with NetApp Controllers
 - Solid State Drives (SSD/SSD-NVMe)
 - MZWLJ3T8HBL5-00AG6 (3.8TB NVMe)
 - MZWLJ15THALA-00AG6 (15.3TB NVMe)
 - XS3840SE70104 (3.8TB SAS SSD)
 - TC58NC1132GTC (3.8TB SAS SSD)
 - XS3840SE70104 (960GB SAS SSD)
 - TC58NC1132GTC (960GB SAS SSD)
 - Hard Drives (SSD/SSD-NVMe)

- ST1800MM0149 (1.8TB SAS HDD)
- WUS721010AL5205 (10TB SAS HDD)
- Search terms specified in [SD-AA]—the evaluation team searched on the following terms:
 - “drive encryption”
 - “disk encryption”
 - “key destruction”
 - “key sanitization”
 - “password caching”
 - “key caching”
 - “opal management software”/ “opal”
 - “sed management software”/ “self encrypting drive”.

The results of these searches did not identify any vulnerabilities that are applicable to 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 assurance activities specified in the claimed Protection Profile. 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 NetApp Volume Encryption: Common Criteria Configuration Guide, Version 1.6, November 7, 2024. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained. It is important to note the excluded functionality listed in Section 5.3 and follow the configuration instructions to ensure that this functionality is disabled.

Evaluation activities are strictly bound by the assurance activities described in the Protection Profile and accompanying Supporting Documents. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11 Security Target

The ST for this product's evaluation is *NetApp Storage Encryption (NSE) running ONTAP 9.14.1 Security Target*, Version 1.7, November 7, 2024 [7].

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

AAR	Assurance Activities Report
AFF	All Flash FAS
AK	Authentication Key
BEV	Border Encryption Value
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CIFS	Common Internet File System
DEK	Data Encryption Key
DHCP	Dynamic Host Configuration Protocol
ETR	Evaluation Technical Report
FAS	Fabric Attached Storage
FC	Fibre Channel
FCoE	Fibre Channel over Ethernet
HA	High Availability
HDD	Hard disk drive
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IT	Information Technology
NAS	Network Attached Storage
NFS	Network File System
NIST	National Institute of Standards and Technology
NSE	Network Storage Encryption
NVMe	Non-Volatile Memory express
OKM	Onboard Key Manager
PCL	Product Compliant List
SAN	Storage Area Network
SAR	Security Assurance Requirement
SED	Self-Encrypting Drive
SFR	Security Functional Requirement
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SSD	Solid state drive
SSH	Secure Shell
ST	Security Target
SVM	Storage Virtual Machine
TCG	Trusted Computing Group
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification

13 Bibliography

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

- [1] 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.
- [2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
- [3] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017.
- [4] Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.
- [5] collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, 1 February 2019.
- [6] Supporting Document – Mandatory Technical Document – Full Drive Encryption: Authorization Acquisition, Version 2.0 + Errata 20190201, 1 February 2019.
- [7] NetApp Storage Encryption (NSE) running ONTAP 9.14.1 Security Target, Version 1.7, November 7, 2024.
- [8] NetApp Storage Encryption: Common Criteria Configuration Guide Version 1.4, November 7, 2024.
- [9] NetApp ONTAP 9.14.1 commands, June 26, 2024.
- [10] NetApp Set up, upgrade and revert ONTAP- ONTAP 9, July 02, 2024.
- [11] Assurance Activities Report for NetApp Storage Encryption (NSE) running ONTAP 9.14.1, Version 1.1, November 8, 2024.
- [12] Evaluation Technical Report for NetApp Storage Encryption (NSE) Running ONTAP 9.14.1 (Leidos Proprietary), Version 1.0, September 25, 2024.
- [13] NetApp Storage Encryption (NSE) running ONTAP 9.14.1 Common Criteria Test Report and Procedures, Version 1.1, 7 November 2024.