Swedish Certification Body for IT Security

Certification Report - PureStorage FlashBlade 4.4.8

Issue: 1.0, 2025-dec-02

Authorisation: Theodora Arvanitidis, Junior Certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is the Purity OS 4.4.8 running on the FlashBlade //E, FlashBlade //S200, and FlashBlade //S500. Pure Storage FlashBlade (FB) provides managed all flash file and object storage. This allows for traditional hierarchical storage where information is accessed based on its path and object storage where data is accessed based on an identifier and associated metadata. FlashBlade provides both the performance advantage of file storage and the scalability advantage of object storage. File store access is supported via NFS/SMB clients and object store access is supported by S3 clients.

The deliverable to a user is the TOE hardware with a base version of the software. The customer recieves the following:

- Two FlashBlade//E chassis with two external fabric (XFM) modules, FlashBlade//S200, and FlashBlade//S500.

- Documentation is available to registered customers on the Pure Storage support site (https://support.purestorage.com/FlashBlade).

The evaluation has been conducted on EAL2.

The ST does not claim conformance to a PP.

The ST includes three threats, no OSPs, and three assumptions.

The evaluation has been performed by Intertek at the Information Technology Security Evaluation and Testing (ITSET) Facility at Intertek EWA-Canada in Ottawa remotely accessing the TOE set up in Puretec Lab Sunnyvale US.

The evaluation was completed on 2025-09-15. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version. 3.1 release 5.

Intertek is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Intertek is also accredited by the Swedish accreditation body according to ISO/IEC 17025 for Common Criteria.

2 Identification

Certification Identification	
Certification ID	CSEC2024007
Name and version of the certified IT product	Purity OS 4.4.8 running on the FlashBlade //E, FlashBlade //S200, and FlashBlade //S500 Models
Security Target Identification	Pure Storage FlashBlade 4.4.8 Security Target, Pure Storage Inc, 2025-10-30, version 3.4
EAL	EAL2
Sponsor	Pure Storage, Inc
Developer	Pure Storage, Inc
ITSEF	Intertek
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	2.6.1
Scheme Notes Release	22.0
Recognition Scope	CCRA, SOG-IS
Certification date	2025-11-21

3 Security Policy

Security Audit

User Data Protection

Identification And Authentication

Security Management

Protection of the TSF

TOE Access

Trusted Path / Channels

3.1 Security Audit

Audit entries are generated for security related events. The audit logs are protected from unauthorized modification, unauthorized deletion, and may be reviewed by authorized administrators. Viewed audit records can be sorted and filtered. Timestamp information is provided to support auditing. An audit log storage duration and record limit are also enforced.

3.2 User Data Protection

The TOE provides managed storage to NFS, SMB, and S3 clients.

3.3 Identification and Authentication

Administrators must identify and authenticate prior to TOE access. The TSF enforces a failure limit and passwords are not revealed during authentication.

3.4 Security Management

The TOE provides management capabilities via a web based GUI (via HTTPS) and CLI (via SSH). Management functions allow the administrators to configure system and network settings, configure users and roles, and perform other TOE functions. The storage administrator (or array administrator) can also configure user access to the array's file and object storage. Access via SMB, S3, and NFS clients is supported.

3.5 Protection of the TSF

Reliable timestamps are provided in support of audit record creation.

3.6 TOE Access

A banner is presented on user login. Administrator sessions can be locked or terminated by both the user and TSF. Establishment of sessions can be restricted to specific IP addresses.

3.7 Trusted Path / Channels

The communications links between the TOE and its remote administrators are protected using HTTPS (TLS v1.2 or TLS v1.3) for the Web GUI or SSH v2 for the CLI. TLS v1.2 is used to protect communication to the remote audit log server. The LDAP connection is protected by TLS v1.2 or TLS v1.3.

4 Assumptions and Clarification of Scope

The [ST] contains three assumptions - two for usage and one for the environment - along with three threats.

4.1 Usage Assumptions

The Security Target makes two assumptions on the usage of the TOE.

A.MANAGE, which assumes that there are one or more competent individuals assigned to manage the TOE.

A.NOEVIL, which assumes that the authorized administrators are not careless, willfully negligent, or hostile.

4.2 Environmental Assumptions

The Security Target makes one assumption on the operational environment of the TOE.

A.LOCATE, which assumes that the TOE and LDAP/AD server will be located within controlled access facilities, which will prevent unauthorized physical access.

4.3 Clarification of Scope

The Security Target contains three threats, which have been considered during the evaluation.

T.ACCOUNT, where an authorized user of the TOE could gain unauthorized access to TOE configuration information or perform operations for which no access rights have been granted.

T.COMPDATA, where an unauthorized individual may attempt to access or alter TSF data or user data stored by the TOE by circumventing security.

T.UNDETECT, where authorized or unauthorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.

The Security Target contains no Organisational Security Policies (OSPs).

5 Architectural Information

The following diagram depicts the TOE components:

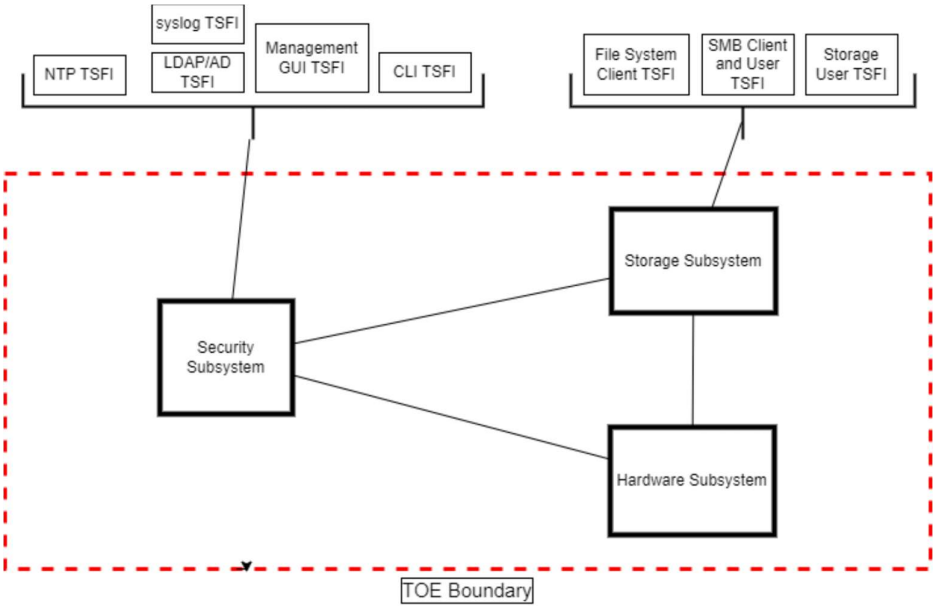

Figure 1 - TOE Architectural Description

The security subsystem is responsible for performing identification and authentication of administrative users, enforcing administrator IP address restrictions, performing role-based access control authorization, managing user access to storage, and creates audit events information. It enforces Web

GUI and CLI session restrictions and ensures that trusted paths and channels are protected. It also manages the connection with a syslog server. The file system SFP, SMB client SFP, SMB share SFP, and object store SFP is also managed through the security subsystem. The security subsystem also maintains system time using the system clock and a NTP server or servers.

The storage subsystem is responsible for storing user data as well as audit data. The storage subsystem is also responsible for the enforcement of the SFPs provided by the security subsystem. This subsystem also ensures that old audit records are deleted.

6 Documentation

The TOE includes the following documentation:

- FlashBlade//E Quick Installation Guide, 40-0323-01
- FlashBlade//E Multi-Chassis Installation Guide, 50-0046-04
- FlashBlade//S Quick Installation Guide, 40-0284-02
- FlashBlade//S Single Chassis Installation Guide, 50-0030-01
- FlashBlade//S Multi-Chassis Quick Installation Guide, 50-0041-01
- FlashBlade//S Multi-Chassis Installation Guide. 50-0040-05
- FlashBlade User Guide Version, 4.4.2
- FlashBlade Command Line Interface Reference, Version 4.4.2
- FlashBlade Object Store S3 REST API 2.3
- FlashBlade 4.4.8.post1 Common Criteria Guidance Supplement

Registered customers can obtain the documentation on the Pure Storage support site.

7 IT Product Testing

7.1 Developer Testing

The developer tested the TSF with full coverage. The developer testing was performed on in between 10 May 2025 to 10 June 2025 at the developer's premises in Sunnyvale US.

The actual results matched the expected results in all of the developers tests, and the evaluator has examined the test evidence and reported that the test results were successful with a clearly identified outcome.

7.2 Evaluator Testing

The evaluator has repeated all the developer's tests in order to gain assurance in the developers testing process. The evaluators devised five independent test cases.

Independent testing was performed at the Information Technology Security Evaluation and Testing (ITSET) Facility at Intertek EWA-Canada in Ottawa remotely accessing the TOE set up in Puretec Lab Sunnyvale US during May 2025. All evaluator testing was performed with the setup in Figures 2 and 3.

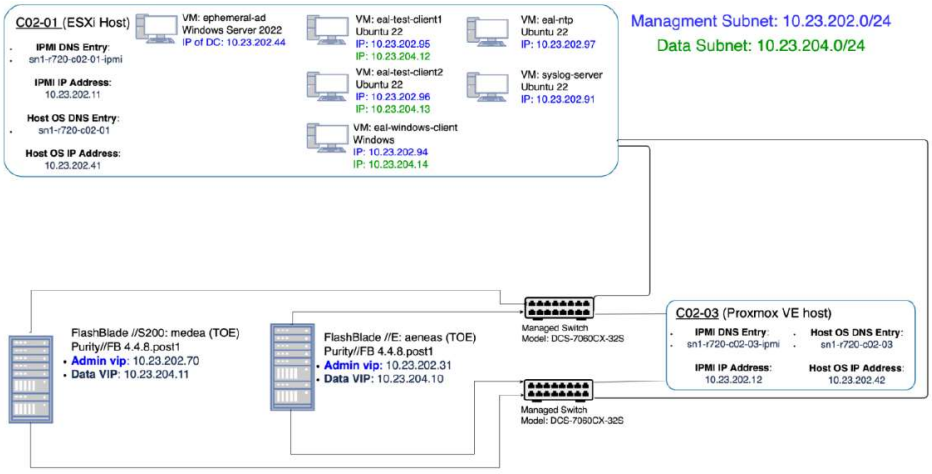

Figure 2 - TOE Test Configuration

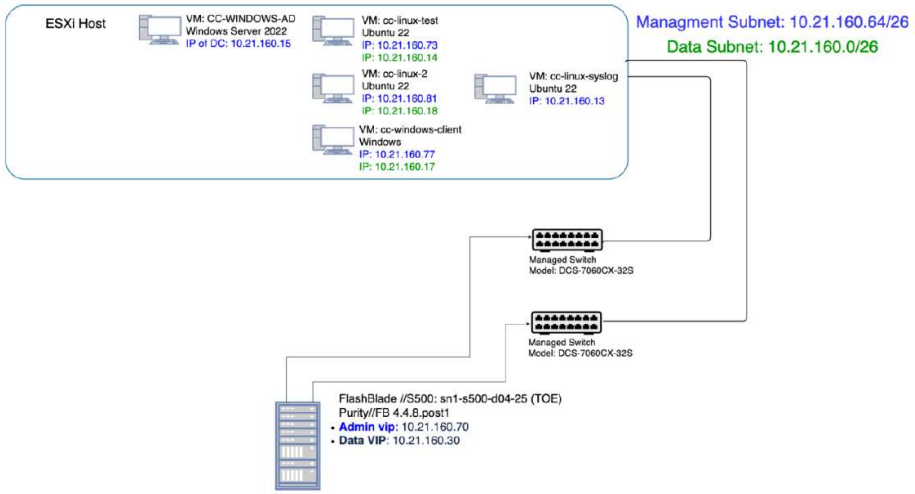

Figure 3 - Hardware and Software

7.3 Penetration Testing

An internet search of potential vulnerabilities and product scanning using several products was used to determine potential vulnerabilities. Penetration testing was performed to verify that these vulnerabilities were not exploitable in the evaluated configuration. Penetration testing focused on the Server component. Penetration testing was performed at the Information Technology Security Evaluation and Testing (ITSET) Facility at Intertek EWA-Canada in Ottawa remotely accessing the TOE set up in Puretec Lab Sunnyvale US during May to July 2025.

8 Evaluated Configuration

The following are requirements on the Operational Environment:

- Administrator Workstation
- LDAP Server or AD Server supporting Kerberos authentication and TLS v1.2 or TLS v1.3
- NTP Server
- Syslog server
- Managed Switch (one per chassis)

The following are requirements on the evaluated configuration:

- The Web GUI used to manage FlashBlade must use TLS v1.2 or TLS v1.3
- Administration using the REST API is disabled by default and shall not be enabled
- Session lockouts must be configured by setting an idle timeout period
- A login banner shall be created
- The FlashBlade 4.4.8. has default users and roles which are intended for use by support personnel and these are not to be used in the evaluated configuration
- A syslog server supporting TLS v1.2 is required since FlashBlade does not support other TLS versions for syslog connections
- The LDAP server must support Kerberos authentication and TLS v1.2 or TLS v1.3. Microsoft Server 2016 and later is compatible. External certificates must be configured. For client Kerberos authentication an encryption type of “aes256-cts-hmac-sha1-96” or better must be used
- Trusted CA and trusted CA signed certificates must be imported as FlashBlade client uses array certificates and external certificates
- Management access is restricted to ssh and the web GUI by removing the network access policy rules granting REST, SNMP and local superuser access

The following features are excluded from the evaluation:

- HTTP access to file systems
- Use of Pure1 Remote Assistance and logging
- Ops Admin role
- Use of the local console interface
- NFS ACLs and ACEs
- Pure file safemode
- Pure object safemode
- S3 object lock
- Bandwidth throttling for replication
- File system usage limits
- File system snapshots
- Fast remove
- Quotas
- Object replication
- File system replication
- Analysis

- Administration using the REST API
- Health monitoring
- Enterprise key management (EKM) servers
- Key management interoperability protocol (KMP)
- Alerts

The following are not supported in the evaluated configuration:
- NFSv4.1 pNFS, Delegation, Referrals, and Share reservation
- SMBv1

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the [ST] for an attack potential of Basic.

The certifier reviewed the work of the evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators' overall verdict is PASS.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class Name / Assurance Family Name	Short name	Verdict
Development	ADV	
Security Architecture	ADV_ARC.1	PASS
Functional Specification	ADV_FSP.2	PASS
TOE Design	ADV_TDS.1	PASS
Guidance documents	AGD	PASS
Operational user guidance	AGD_OPE.1	PASS
Preparative procedures	AGD_PRE.1	PASS
Life-cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.2	PASS
CM Scope	ALC_CMS.2	PASS
Delivery	ALC_DEL.1	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security Objectives	ASE_OBJ.2	PASS
Extended Components Definition	ASE_ECD.1	PASS
Security Requirements	ASE_REQ.2	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.1	PASS
Functional Tests	ATE_FUN.1	PASS
Independent Testing	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

CC	The Common Criteria
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TOE	Target of Evaluation

12 Bibliography

[ST]
Pure Storage FlashBlade 4.4.8 Security Target, Pure Storage Inc, Intertek, version 3.4 2025-10-30, FMV ID 24FMV3395-35

[CC/CEM]
Common Criteria for Information Technology Security Evalua-tion, Version 3.1, revision 5, April 2017. Parts 1-3.
Common Methodology for Information Technology Security Evaluation, Version 3.1, revision 5, April 2017.

[FER]
FINAL EVALUATION REPORT FOR PURE STORAGE, INC. PURITY OS 4.4.8 RUNNING ON THE FLASHBLADE //E, FLASHBLADE //S200, OR FLASHBLADE //S500 MOD-ELS, Pure Storage Inc, Intertek, version 1.2 2025-11-14, FMV ID 24FMV3395-35

[AGD]
Pure Storage FlashBlade 4.4.8.post1 Common Criteria Guidance Supplement version 1.2, Pure Storage Inc, Intertek, 2025-10-30, FMV ID 24FMV3395-35

[AGD1]
FlashBlade User Guide Version 4.4.2, Pure Storage Inc, Intertek, FMV ID 24FMV3395-25

[AGD2]
FlashBlade Command Line Interface Reference Version 4.4.2, Pure Storage Inc, Intertek, FMV ID 24FMV3395-25

[AGD3]
FlashBlade Object Store S3 REST API Version 2.3, Pure Storage Inc, Intertek, FMV ID 24FMV3395-25

[AGD4]
FlashBlade//E Quick Installation Guide 40-0323-01, Pure Storage Inc, Intertek, FMV ID 24FMV3395-25

[AGD5]
FlashBlade//E Multi-Chassis Installation Guide 50-0046-04, Pure Storage Inc, Intertek, FMV ID 24FMV3395-25

[AGD6]
FlashBlade//S Quick Installation Guide 40-0284-02, Pure Storage Inc, Intertek, FMV ID 24FMV3395-25

[AGD7]
FlashBlade//S Single Chassis Installation Guide 50-0030-01, Pure Storage Inc, Intertek, FMV ID 24FMV3395-25

[AGD8]
FlashBlade//S Multi-Chassis Quick Installation Guide 50-0041-01, Pure Storage Inc, Intertek, FMV ID 24FMV3395-25

[AGD9]
FlashBlade//S Multi-Chassis Installation Guide 50-0040-05, Pure Storage Inc, Intertek, FMV ID 24FMV3395-25

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
2.6.1	2025-10-16	None
2.6	Application	Original version

A.2 Scheme Notes

The following Scheme Notes have been considered during the evaluation:

- Scheme Note 15 - Testing
- Scheme Note 18 - Highlighted Requirements on the Security Target
- Scheme Note 22 - Vulnerability Assessment
- Scheme Note 27 - ST requirements at the time of application for certification
- Scheme Note 28 - Updated procedures for application, evaluation and certification