PURESTORAGE®

WHITE PAPER | OCTOBER 2025 | VERSION 1.2

Security and Compliance Assurance Packet

Prepared by the Pure Storage Global Information Security Office (GISO)

Contents

Welcome from the CISO 3

About Pure Storage 4

- Threat Modeling 5
- Peer Code Reviews 5
- Security Design Reviews 5
- Continuous Security Testing 5
- Compliance and Governance 5

Product Security: Trusting Us with Your Data 5

- Cloud Security: Protecting Data in the Pure1 Platform and Portworx Cloud Products 5
- Platform Security: Protecting Data in FlashArray and FlashBlade Systems 6
- Media Sanitization 7
- Secure Software Development 7
- Vulnerability Reporting and Responsible Disclosure 7

Encryption: Why Security from Pure Storage Stands Out 7

- Data in Transit 7
- Data at Rest 7

Enterprise Security: Information Security Program 8

- Identity and Access Management 8
- Enterprise Resiliency 8
- Risk Management and Incident Response 9
- Secure Infrastructure and Operations 9
- Scanning 9
- Hardening 10
- Internal Testing 10
- Penetration Testing 10
- Security Awareness and Training 10

AI Governance Executive Summary 11

- AI Governance Model 11
- Enterprise AI Data Protection 11
- Commitment to Trust and Innovation 11

Data Centers 12

Certifications: Governance, Risk, and Compliance 12

- NIST FIPS 140-3 12
- NIAP Common Criteria 14
- ISO 27001 Certification 15
- SOC 2 Program 16
- TAA/NDAA Certification 17
- M-22-18Attestations 18
- Cyber Insurance Coverage 20

Get in Touch 21

- Resources and Contact Information 21

Welcome from the CISO

Thank you for your interest in Pure Storage®. Pure Storage delivers the industry's most advanced data storage platform, designed to store, manage, and protect the world's data at any scale. From AI to archive, Pure Storage provides a unified cloud experience with one storage-as-a-service platform across on-premises, cloud, and hosted environments presented with one comprehensive dashboard. Our technology is built on the proven, non-disruptive Evergreen® architecture.

By helping organizations save time, money, and energy, it's no surprise that leading brands choose Pure Storage and that it boasts the highest Net Promoter Score (NPS) of 82 in the industry. Pure Storage has been recognized 11 times as A Leader in Gartner® Magic Quadrant™ for Primary Storage Platforms[1], underscoring its strong market performance and innovative approach in enterprise flash storage. We are also proud to be recognized in the Fortune Best Workplaces in Technology list for four consecutive years. This has also been my personal experience.

At Pure Storage, we focus on creating innovative solutions that drive extraordinary customer experiences and meaningful results, ultimately helping build a better world with data. Security, privacy, and compliance are core principles in developing, delivering, and supporting our products and services. Our defense-in-depth security program has been validated by independent third-party auditors, and we maintain resiliency capabilities through purpose-built security programs. Our globally distributed security program operates 24/7/365, continuously protecting our infrastructure and supporting our customers.

Attached is information about our security program, certifications, and strategy, including how we protect your critical data resources. We hope this Assurance Packet will provide clarity on many aspects of our security approach.

Thank you for the opportunity to earn your trust.

Best regards,

Rick Orloff
VP, Chief Information Security Officer

About Pure Storage

Pure Storage (NYSE: PSTG) delivers the industry's most advanced data storage platform to store, manage, and protect the world's data at any scale. With Pure Storage, organizations have ultimate simplicity and flexibility, saving time, money, and energy. From AI to archive, Pure Storage delivers a cloud experience with one unified storage-as-a-service platform across on-premise, cloud, and hosted environments.

Our platform is built on our Evergreen architecture that evolves with your business—always getting newer and better with zero planned downtime, guaranteed. Our customers are actively increasing their capacity and processing power while significantly reducing their carbon and energy footprint.

Security by Design

At Pure Storage, the "Security by Design" principle is executed through a continuous loop integrating security at every phase of the software development lifecycle (SDLC), ensuring a resilient product capable of withstanding cyber threats. This strategy involves various comprehensive procedures and consistent updates.

Threat Modeling

This crucial step involves identifying potential security threats early in the development process, using methods such as the STRIDE framework. It helps establish a risk-based security baseline and aligns security features with the identified risks. Threat models are continuously updated and maintained to address any residual risks before the release.

Peer Code Reviews

As part of our Secure SDLC, all code changes undergo peer code reviews. These reviews help identify potential security vulnerabilities and ensure our code complies with secure coding standards.

Security Design Reviews

New software or changes that could alter the threat model or introduce new security implications undergo a thorough security design review before deployment.

Continuous Security Testing

Our development teams use various security tools such as dynamic application security testing (DAST), open source scanning (SCA), vulnerability assessment tools, and penetration testing. The results from these security tests are reviewed through our Governance, Risk, and Compliance process.

Compliance and Governance

The software development practices at Pure Storage adhere to NIST Secure Software Development Framework (NIST SP 800-218). See our M-22-18 attestation covering FlashArray™, FlashBlade®, and Portworx® family of products.

Product Security: Trusting Us with Your Data

At Pure Storage, security is at the core of everything we do. Whether managing data in the Pure1® cloud platform, securing Kubernetes environments with Portworx, or protecting enterprise workloads on FlashArray and FlashBlade, we have always-on encryption, compliance with leading security frameworks, and advanced data protection.

Cloud Security: Protecting Data in the Pure1 Platform and Portworx Cloud Products

Pure Storage ensures that data within the Pure1 platform and Portworx cloud products are protected using enterprise-grade security controls, which are independently certified and compliant with:

- SOC 2 Type II reports, covering Security, Confidentiality, and Availability controls
- Aligns with ISO 27001 standards for cloud security governance

Pure Storage cloud services are hosted in AWS, whose data centers are certified and compliant with:

- **SOC2 Type II**: Covers Security, Confidentiality, and Availability controls, ensuring stringent safeguards for customer data
- **ISO 14001**: Establishes environmental management standards to help reduce the ecological impact of AWS data centers while ensuring regulator compliance
- **ISO 22301**: Provides a business continuity management system (BCMS) to ensure AWS services remain resilient against disruptions and disasters
- **ISO 27001**: Aligns with cloud security governance best practices, providing a framework for risk management and continuous improvement
- **ISO 50001**: Focuses on energy efficiency and sustainability, helping AWS optimize power consumption in data centers and improve environmental performance
- **CSA STAR Level 2**: Certifies cloud security best practices through independent third-party audits, ensuring AWS meets comprehensive risk management and compliance benchmarks
- **NIST 800-53**: Defines security and privacy controls for U.S. federal information systems, ensuring AWS adheres to strict government security standards

The Pure1 Platform: Secure Cloud-based Management

Pure1, our cloud-based AI-driven storage management and analytics platform, ensures secure communications, encrypted data storage, and compliance with strict security standards.

Portworx: Cloud-native Data Protection for Kubernetes

Portworx delivers enterprise-grade storage, backup, and data management for Kubernetes, ensuring stateful applications remain highly available, resilient, and secure across clouds and on-premise environments.

Platform Security: Protecting Data in FlashArray and FlashBlade Systems

FlashArray: Secure Storage for Enterprise Workloads

- Data encryption is always enabled for both data at rest and in transit. Data protocol encryption is also available for SMTP, DNS, NFS, and SMB protocols as well as replication. Our AES-256 encryption protects data and communications.
- Authentication using SAML or AD/LDAP, authorization through role-based access controls (RBAC), and comprehensive auditing logs are available.
- FIPS 140-3-validated and NIAP/Common Criteria certified, meeting the highest security standards.

FlashBlade: High-performance Encryption for Unstructured Data

- Data encryption is always enabled for both data at rest and in transit. Data protocol encryption is also available for S3, NFS, and SMB protocols. Our AES-256 encryption protects data and communications.
- Authentication using SAML or AD/LDAP, authorization through role-based access controls (RBAC), and comprehensive auditing logs are available.
- FIPS 140-3-compliant and under test for Common Criteria

Media Sanitization

Pure Storage partners with third-party security firms to validate our sanitization feature conforms with NIST SP 800-88 Rev1. Conformance reports are available upon request.

Secure Software Development

Conformance to OMB M-22-18 & NIST SP 800-218A

Pure Storage attests to compliance with OMB M-22-18, confirming adherence to NIST SP 800-218A (Secure Software Development Framework—SSDF). This attestation is officially logged with the U.S. Government and is required for continued engagement with U.S. federal agencies.

Key principles followed under SSDF include:

- Risk-based secure SDLC practices
- Software supply chain security, including integrity verification, provenance tracking, and dependency management
- Continuous monitoring and vulnerability management, integrating security testing, automated scanning, and third-party dependency validation

These measures ensure Pure Storage's software development aligns with federal security requirements, reducing the risk of supply chain attacks and software vulnerabilities.

Vulnerability Reporting and Responsible Disclosure

Please see our Vulnerability Reporting and Disclosure Policy for details.

At Pure Storage, we believe in transparency and accountability. We are committed to publishing to our Pure Storage Common Vulnerabilities and Exposures (CVE) Database (login required) for known security vulnerabilities; typically 90 days after a fix is made available to our customers. This is to provide our customers with the opportunity to safely upgrade and/or apply necessary patches prior to a public notification. Pure Storage may also issue interim workarounds for critical vulnerabilities that require a longer remediation timeframe. Pure Storage reserves the right to make exceptions to this policy when necessary.

Encryption: Why Security from Pure Storage Stands Out

Pure Storage employs robust encryption mechanisms to ensure data security across our enterprise, products, and services we provide to our customers. We continuously evaluate our cryptographic posture to ensure it aligns with best practices and regulatory requirements.

Pure partners with independent third-party entities to validate our posture through our FIPS 140-3, SOC2 and ISO 27001 certification programs. See the ISO 27001 Certification section below.

Data in Transit

Pure Storage secures data transmission by requiring TLS 1.2 or above, preventing unauthorized access and ensuring the integrity of data moving between systems.

Data at Rest

All data is protected using Advanced Encryption Standard (AES) 256-bit encryption. This encryption is always on, ensuring data security.

Enterprise Security: Information Security Program

At Pure Storage, protecting our customers' data, and the security of our information assets, is a top priority. Our Information Security Program is designed to engage core security standards, safeguard critical business information, and maintain trust with our customers and partners. We've achieved ISO 27001 certification, demonstrating our commitment to maintaining an information security management program that meets or exceeds international standards.

Identity and Access Management

The Pure Storage Identity and Access Management (IAM) Program is a centralized team for providing continuous direction and oversight for identity and access across Pure Storage infrastructure. The program is designed to enhance security, establish compliance, and provide seamless identity management for customers, partners, and employees. Key features include:

Centralized access management

- The program consolidates identity management across Pure internally and provides guidance for customer-facing services, ensuring timely provisioning and deprovisioning.

Principle of least privilege (PoLP)

- Role-based access control (RBAC) ensures effective privilege is based on functional roles.
- Privileged access must be explicitly approved, regularly reviewed, and documented.
- Separation of duties is enforced to minimize the risk of unauthorized privilege escalation.

Multi-factor authentication (MFA) and single sign-on (SSO)

- Business applications leverage SSO though Okta which provides strong authentication policies aligned with NIST SP800-63B, including risk-based step-up to MFA.
- Posture checks ensure that only trusted clients are allowed into critical applications.

Threat detection

- Identity-related activity is reviewed and analyzed against common threats and anomalous behavior.

The program, coupled with a highly skilled team of professionals, ensures a secure, efficient, and centralized approach to identity management, reinforcing the security posture of the Pure Storage enterprise environment.

Enterprise Resiliency

The Pure Storage Enterprise Resiliency Program takes responsibility for the development, implementation, exercising, and documentation of business continuity, disaster recovery, and crisis/incident management, striving to ensure alignment with best practices and industry standards.

Pure Storage program aligns with the following regulatory requirements and standards:

- **ISO 22301:2019:** Business continuity management systems
- **NIST Cybersecurity Framework:** Guidelines for improving critical infrastructure cybersecurity
- **NIST SP 800:** Special publications addressing cybersecurity best practices
- **BCI Good Practices Guidelines:** Best practices for business continuity and resilience

Risk Management and Incident Response

Our risk management strategy, consistent with ISO 27001, includes regular risk assessments, security audits, and real-time monitoring of potential threats.

At Pure Storage, we maintain a proactive risk management and incident response framework to safeguard our operations, customers, and data. Our approach aligns with ISO 27001, NIST Cybersecurity Framework (CSF), and industry best practices.

Risk Management Approach

- Regular assessments identify and evaluate risks based on likelihood and impact.
- Risks are categorized and managed using one of four strategies: avoid, transfer, accept, or mitigate.
- The Risk Register, maintained by the Governance, Risk, and Compliance (GRC) team, ensures risks are continuously monitored and reviewed quarterly, depending on severity.

Incident Response Framework

Our Incident Response Program operates 24/7/365 to detect, contain, and mitigate security incidents. We follow the NIST 800-61 Incident Handling Guide, with a structured response process:

- **Preparation:** Regular security training, tabletop exercises, and penetration testing
- **Detection and analysis:** Real-time threat monitoring and automated endpoint protection
- **Containment and Eradication:** Rapid incident containment, forensic investigation, and threat removal
- **Recovery and Lessons Learned:** Secure system restoration, post-incident review, and policy updates

By integrating continuous risk monitoring, real-time incident response, and enterprise-wide resilience, Pure Storage ensures the highest level of data protection and security readiness.

Secure Infrastructure and Operations

We continuously monitor and protect our infrastructure to defend against evolving threats:

- Network and endpoint security to detect and respond to unauthorized access attempts
- Regular penetration testing to identify and remediate vulnerabilities
- Secure mobile device management (MDM) to enforce security policies on all connected devices

Scanning

Pure Storage uses a systematic approach to enterprise-level scanning to maintain security and compliance. This includes utilizing various tools and processes such as code scanning (SAST), infrastructure and network monitoring, threat intelligence, attack surface management, and vulnerability scanning. The security program is comprehensive, ensuring rapid remediation of identified vulnerabilities and adhering to industry standards like NIST Cybersecurity Framework and ISO 27001.

Hardening

Pure Storage enforces specific security standards during the hardening process, such as infrastructure security requirements, which include removing or disabling unused networking services, providing configuration guides, and using tools like Tenable for vulnerability scanning. Additionally, we employ technical measures like configuration hardening following CIS benchmarks, using firewalls, conducting regular security testing, and ensuring compliance with security standards like FIPS and Common Criteria. These measures help maintain system security and ensure resources remain protected from potential threats.

System Hardening

Pure Storage ensures system hardening through several critical steps to enhance security and protect against vulnerabilities:

- We remove or disable unused networking and computing services, such as finger, rlogin, FTP, and simple TCP/IP services, reducing the attack surface.
- We install a system firewall, TCP wrappers, or similar technology to monitor and control network traffic and restrict access based on IP addresses.
- We provide configuration guides with detailed hardening information for various operating systems, offering step-by-step security instructions. We also deploy vulnerability scanning and host-checking capabilities to identify and address security weaknesses and drive compliance with security policies.

These comprehensive measures help Pure Storage maintain and update the security of its systems, ensuring all information resources are protected against potential threats.

Internal Testing

At Pure Storage, our Internal Testing & Quality Assurance (QA) program spans the entire product line and code base to ensure software and hardware releases meet strict quality, security, and reliability standards. Our QA teams execute full test suites alongside industry benchmarks, ensuring comprehensive validation before deployment.

This process has contributed to six nines (99.9999%) uptime/availability across all installed products. To maintain this reliability, Pure Storage performs continuous regression testing, verifying that both the latest releases and three prior generations of software and hardware remain free from availability or performance issues.

Our hardware testing process includes:

- Real-time quality monitoring and management
- Extensive automated quality assurance and testing
- Continuous 48-hour load testing on all input/output (I/O) devices

Penetration Testing

The security team partners with independent third-party vendors to perform specialized penetration tests across our infrastructure, products, and services including FlashArray, FlashBlade, and cloud environments. Tests cover web applications, product features, code reviews, and threat modeling thereby driving a robust security posture.

Security Awareness and Training

At Pure Storage, we believe that strong security starts with informed and vigilant employees. We are committed to fostering a culture of cybersecurity awareness that empowers our workforce to protect sensitive data and safeguard our company's resources.

As part of our comprehensive Security Awareness Program, all employees undergo mandatory annual security training designed to reinforce best practices, educate on emerging threats, and equip individuals with the knowledge needed to maintain a secure digital environment.

In addition to our standard training, we provide targeted, role-specific security education to ensure that employees handling sensitive information or performing high-risk tasks receive tailored guidance and advanced protection strategies. We also host an internal hackathon annually.

By investing in continuous security education, we ensure that every member of our team, from new hires to executives, plays a crucial role in strengthening our security posture. Cybersecurity is not just a responsibility; it's a shared commitment to excellence, trust, and innovation.

AI Governance Executive Summary

At Pure Storage, we are committed to the responsible and secure use of GenAI technologies. Our AI Governance framework ensures that deployed AI tools within our enterprise meet legal, security, compliance, and ethical standards, aligning with our core principles of trust, transparency, and data protection.

AI Governance Model

Our AI governance framework includes:

- **Security and compliance review**: AI tools should undergo rigorous security assessments to ensure compliance with industry regulations and internal policies.
- **Data protection assurance**: AI tools utilized within Pure Storage do not train on user prompts, ensuring that enterprise data remains within our controlled environment and is not exposed to external models.
- **Ethical AI review**: We evaluate AI tools for fairness, bias mitigation, and ethical considerations to uphold responsible AI usage.
- **Ongoing monitoring and auditing**: AI tools are regularly monitored for adherence to governance policies.

Enterprise AI Data Protection

Enterprise AI data protection at Pure Storage includes:

- **No data leakage**: AI tools are configured to limit outbound data transmission beyond our secured environment.
- **Access controls**: RBAC, SSO, and MFA requirements ensure that only authorized personnel can utilize AI tools, mitigating risk.
- **Transparency and accountability**: AI tool usage may include logging and audits to maintain visibility into the interactions and decision-making.

Commitment to Trust and Innovation

Our AI governance framework reflects our dedication to maintaining trust while fostering innovation. By implementing robust controls and best practices, Pure Storage ensures that AI enhances operational efficiency without compromising security, privacy, or ethical integrity.

Data Centers

Pure Storage operates resilient data centers in multiple countries to ensure continuous operations amidst potential disruptions. These data centers provide redundancy and robust disaster recovery capabilities to support Pure Storage business operations and the development of products and services.

Certifications: Governance, Risk, and Compliance

NIST FIPS 140-3

Pure Storage aligns to the National Institute of Standards and Technology (NIST) cybersecurity framework for information protection. We meet the listed standards through the NIST FIPS 140-3 Cryptographic Module Validation Program.

Pure Storage Cryptographic Module Validation Listings

Purity Encryption Module is a standalone cryptographic module for the Purity Operating Environment for FlashArray (Purity//FA). Purity//FA powers Pure Storage's FlashArray family of products which provide economical all-flash storage. Purity Encryption Module enables FlashArray to support always-on, inline encryption of data with an internal key management scheme that requires no user intervention.

FIPS 140-3 Certificate 4937

https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4937

Certificate #4937

Details

Module Name	Purity Encryption Module	
Standard	FIPS 140-3	
Status	Active	
Sunset Date	1/5/2030	
Overall Level	1	
Caveat	No assurance of the minimum strength of generated SSPs (e.g., keys); No assurance of minimum security of SSPs (e.g., keys, bit strings) that are externally loaded, or of SSPs established with externally loaded SSPs.	
Security Level Exceptions	• Physical security: N/A • Non-invasive security: N/A • Mitigation of other attacks: N/A	
Module Type	Software	
Embodiment	Multi-Chip Stand Alone	
Description	Purity Encryption Module is a standalone cryptographic module for the Purity Operating Environment for FlashArray (Purity//FA). Purity//FA powers Pure Storage's FlashArray family of products which provide economical all-flash storage. Purity Encryption Module enables FlashArray to support always-on, inline encryption of data with an internal key management scheme that requires no user intervention.	
Tested Configuration(s)	• Purity OS 6.4 running on FlashArray X20R3 with Intel Xeon Silver 4210R with PAA • Purity OS 6.4 running on FlashArray X20R3 with Intel Xeon Silver 4210R without PAA	
Approved Algorithms	AES-CTR	A4396
	AES-ECB	A4396
	AES-KW	A4396
	Counter DRBG	A4396
	HMAC-SHA2-256	A4396
	SHA2-256	A4396
Software Versions	FA-1.5	

FIPS 140-2 Certificate 4109:

https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4109

Certificate #4109

Details

Module Name	Purity Encryption Module
Standard	FIPS 140-2
Status	Active
Sunset Date	9/21/2026
Overall Level	1
Caveat	None
Security Level Exceptions	• Design Assurance: Level 2
Module Type	Software-Hybrid
Embodiment	Multi-Chip Stand Alone
Description	Purity Encryption Module is a standalone cryptographic module for the Purity Operating Environment for FlashArray (Purity//FA). Purity//FA powers Pure Storage's FlashArray family of products which provide economical all-flash storage. Purity Encryption Module enables FlashArray to support always-on, inline encryption of data with an internal key management scheme that requires no user intervention.
Tested Configuration(s)	• Purity OS 5.3 running on C60 with Intel Xeon 6130 with PAA • Purity OS 5.3 running on M70R2 with Intel Xeon E5-2698 v4 with PAA • Purity OS 5.3 running on X70R3 with Intel Xeon 6230 with PAA • Purity OS 6.1 running on C60 with Intel Xeon 6130 with PAA • Purity OS 6.1 running on X20R2 with Intel Xeon 4114 with PAA • Purity OS 6.1 running on X70R3 with Intel Xeon 6230 with PAA • Purity OS 6.2 running on XL170 with Intel Xeon 8368 with PAA • Purity OS 6.3 running on XL170 with Intel Xeon 8368 with PAA (single-user mode)
Approved Algorithms	AES — Cert. #A727 CKG — vendor affirmed DRBG — Cert. #A727 HMAC — Cert. #A727 KTS — AES Cert. #A727 SHS — Cert. #A727
Allowed Algorithms	NDRNG
Hardware Versions	Intel Xeon E5-2698 v4, Intel Xeon 4114, Intel Xeon 6130, Intel Xeon 6230 and Intel Xeon 8368
Software Versions	1.3

NIAP Common Criteria

FlashArray running Purity 6.5 is officially certified under the NIAP Common Criteria Protection Profile for Network Devices Version 2.2e, meeting rigorous security standards. This certification validates that FlashArrays running Purity 6.5 have undergone comprehensive third-party testing and meets strict government-grade security requirements. Customers can trust Purity 6.5 to deliver strong, independently verified protection for their most sensitive data.

NIAP Compliant Product Listing

https://www.niap-ccevs.org/products/11525

National Information Assurance Partnership

Common Criteria Certificate

is awarded to

Pure Storage, Inc.

for

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

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 3.1) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. 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 adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Date Issued: 2025-03-27
Validation Report Number: CCEVS-VR-VID11525-2025
CCTL: Advanced Data Security

Assurance Level: PP Compliant
Protection Profile Identifier:
collaborative Protection Profile for Network Devices Version 2.2e

Original Signed By

Director, Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

ISO 27001 Certification

ISO/IEC 27001 is the internationally recognized standard for Information Security Management Systems (ISMS), designed to help organizations protect sensitive data through a structured risk management approach. It provides a framework for identifying, assessing, and mitigating security risks while ensuring compliance with legal and regulatory requirements. By focusing on confidentiality, integrity, and availability of information, ISO 27001 helps organizations establish robust security policies, implement effective controls, and continuously improve their security posture.

COALFIRE CERT

CERTIFICATE NUMBER:
2022-110301

CERTIFICATE OF REGISTRATION

Information Security Management System – ISO/IEC 27001:2022

Coalfire Certification, Inc. certifies that the following organization operates an Information Security Management System (ISMS) that conforms to the requirements of ISO/IEC 27001:2022 per the scope and boundaries statement detailed below:

COMPANY:	Pure Storage, Inc.	ADDRESS:	2555 Augustine Drive Santa Clara, CA 95054 United States

Scope:

The certificate scope comprises the Information Security Management System implemented at Pure Storage. The organizational scope includes our Enterprise controls supporting Pure Storage (Portworx Central, Portworx Enterprise, Portworx Backup). The departmental scope includes the Digital Transformation Group (Enterprise IT), Global Information Security Office (Security Governance and Operations), Infrastructure Shared Services (Engineering Infrastructure), Product Security Incident Response (PSIRT), and Portworx teams affecting the ISMS. These activities are governed by the implemented controls in accordance with the organizational Statement of Applicability.

STATEMENT OF APPLICABILITY:
VERSION: 1.5
DATE: June 13, 2025

Original Registration Date:
November 3, 2022
Certificate Issuance Date:
October 22, 2025
Expiration Date:
November 3, 2028

ON BEHALF OF COALFIRE CERTIFICATION, INC.

Booker Young, VP of Global Assurance

COALFIRE ISO 27001 CERTIFIED CERT

ANAB ANSI National Accreditation Board ACCREDITED ISO/IEC 17021-1 MANAGEMENT SYSTEMS CERTIFICATION BODY

This certificate relates to the Information Security Management System, and not to the products or services of the certified organization. The certification reference number, the mark of the certification body and/or the accreditation mark may not be shown on products or stated in documents regarding products or services. Promotional material, advertisements or other documents showing or referring to this certificate, the trademark of the certification body, or the accreditation mark, must comply with the intention of the certificate.

12735 Morris Road, Suite 250 | Alpharetta, GA 30004 | United States | CoalfireCertification.com

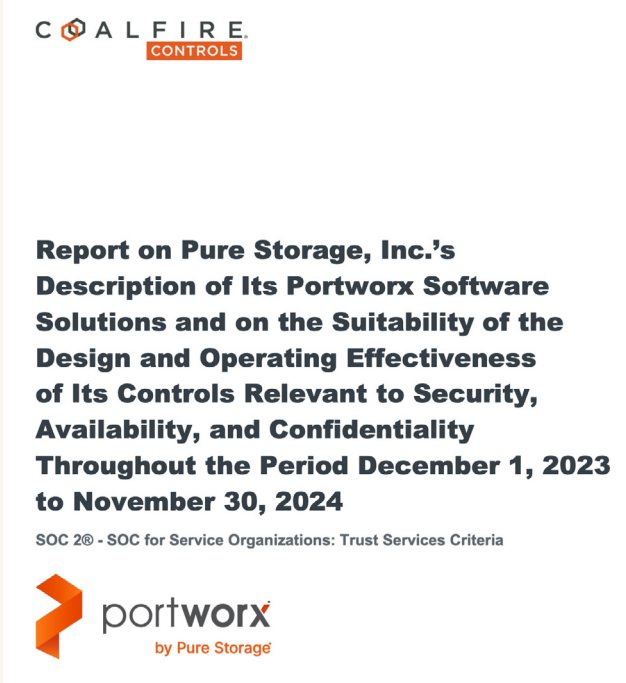
SOC 2 Program

System and Organization Controls (SOC) is a suite of audit reports defined by the American Institute of Certified Public Accountants (AICPA), intended for use by service organizations to issue validated reports of internal controls over those information systems to the users of those services.

Pure Storage undergoes an annual independent assessment to ensure the effectiveness of its controls. Our SOC 2 report details how we maintain the security, confidentiality, and availability of our platform.

Pure Storage Pure1 Cloud SOC 2 Type II

Pure Storage Portworx SOC 2 Type II



TAA/NDAA Certification

Date: January 1, 2025

Pure Storage, Inc. ("Pure Storage") is compliant in the System for Award Management (SAM) www.SAM.gov. In addition, Pure Storage provides the following certifications:

COMMERCIAL PRODUCT CERTIFICATION

Pure Storage certifies that all products and services are newly manufactured, are of a type customarily used by the general public or by non-governmental entities for purposes other than governmental purposes, are sold, leased, or licensed in the course of normal business operations to the general public and are defined as Commercially available off-the-shelf (COTS) item pursuant to FAR 2.101 DEFINITION OF WORDS AND TERMS.

TRADE AGREEMENTS CERTIFICATE

Pure Storage certifies that each end product is a U.S. made end product, a designated country end product, a Caribbean Basin country end product, a Canadian end product, or a Mexican end product as defined in the FAR clause 52.225-5 TRADE AGREEMENTS.

PRODUCTION POINT

Pure Storage production point for end product(s): 8303 Fallbrook Drive, Houston, TX 77064

REPRESENTATION REGARDING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT

Pure Storage does not provide covered telecommunications equipment or services and does not use the covered equipment or services as a substantial or essential component of any system, or as critical technology as part of any system of its offered products or services as defined in the FAR clause 52.204-25.

REPRESENTATION REGARDING PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES

Pure Storage does not provide Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities as defined in the FAR clause 52.204-23.

REPRESENTATION REGARDING APPLICABILITY OF FedRAMP

Pure Storage hereby confirms that it is not a Public Cloud Provider and does not host or have read or write access to the End User data stored on the Products. Further, End User data stored on the Products is not accessed, transmitted or provided to Pure or any third party as part of the Pure1 Reports.

M-22-18Attestations

Pure Storage is compliant with OMB M-22-18, confirming adherence to NIST SP 800-218A (Secure Software Development Framework—SSDF). It specifies the products covered (e.g., FlashArray, FlashBlade, and Portworx) and mentions that this attestation ensures adherence to secure software practices, including regular updates and consistent implementation of cybersecurity measures.

FlashArray and FlashBlade

Docusign Envelope ID: 767AA74A-BB8C-4A14-BD2A-493D91638FFF

OMB Control #: 1670-0052
Expiration Date: 03/31/2027

Secure Software Development Attestation Form
Version 1.0

Section I

☒ **New Attestation** ☐ **Attestation Following Extension or Waiver** ☐ **Revised Attestation**

Type of Attestation: ☐ Company-wide ☐ Individual Product ☒ Multiple Products or Specific Product Version(s) (please provide complete list)

If this attestation is for an individual product or multiple products, provide the software name, version number, and release/publish date to which this attestation applies. Additional pages can be attached to this attestation if more lines are needed:

Product(s) Name	Version Number[4] (if applicable)	Release/Publish Date (if applicable)
FlashArray - Purity		
FlashBlade -Purity		

For the above specified software, this form does not cover software or any components of that software that fall into the following categories:

1. Software developed by Federal agencies;
2. Open source software that is freely and directly obtained directly by a Federal agency;
3. Third-party open source and proprietary components that are incorporated into the software end product used by the agency; or
4. Software that is freely obtained and publicly available.

Note: In signing this attestation, software producers are attesting to adhering to the secure software development practices outlined in Section III for code developed by the producer.

Section II

1. Software Producer Information

Company Name: Pure Storage, Inc.
Address: 2555 Augustine Drive
City: Santa Clara, CA 95054
www.purestorage.com

[4] Attestations are binding for future versions of the named software product unless and until the software producer notifies the agencies to which it previously submitted the form that its development practices no longer conform to the required elements specified in the attestation.

5

Portworx

Docusign Envelope ID: EAACAFC4-A0CC-4C27-987C-18E2CE79CC3A

OMB Control #: 1670-0052
Expiration Date: 03/31/2027

Secure Software Development Attestation Form
Version 1.0

Section I

☑ **New Attestation** ☐ **Attestation Following Extension or Waiver** ☐ **Revised Attestation**

Type of Attestation: ☐ Company-wide ☐ Individual Product ☑ Multiple Products or Specific Product Version(s) (please provide complete list)

If this attestation is for an individual product or multiple products, provide the software name, version number, and release/publish date to which this attestation applies. Additional pages can be attached to this attestation if more lines are needed:

Product(s) Name	Version Number[4] (if applicable)	Release/Publish Date (if applicable)
Portworx Enterprise		
Portworx Backup		
Portworx Data Services		

For the above specified software, this form does not cover software or any components of that software that fall into the following categories:

1. Software developed by Federal agencies;
2. Open source software that is freely and directly obtained directly by a Federal agency;
3. Third-party open source and proprietary components that are incorporated into the software end product used by the agency; or
4. Software that is freely obtained and publicly available.

Note: In signing this attestation, software producers are attesting to adhering to the secure software development practices outlined in Section III for code developed by the producer.

Section II

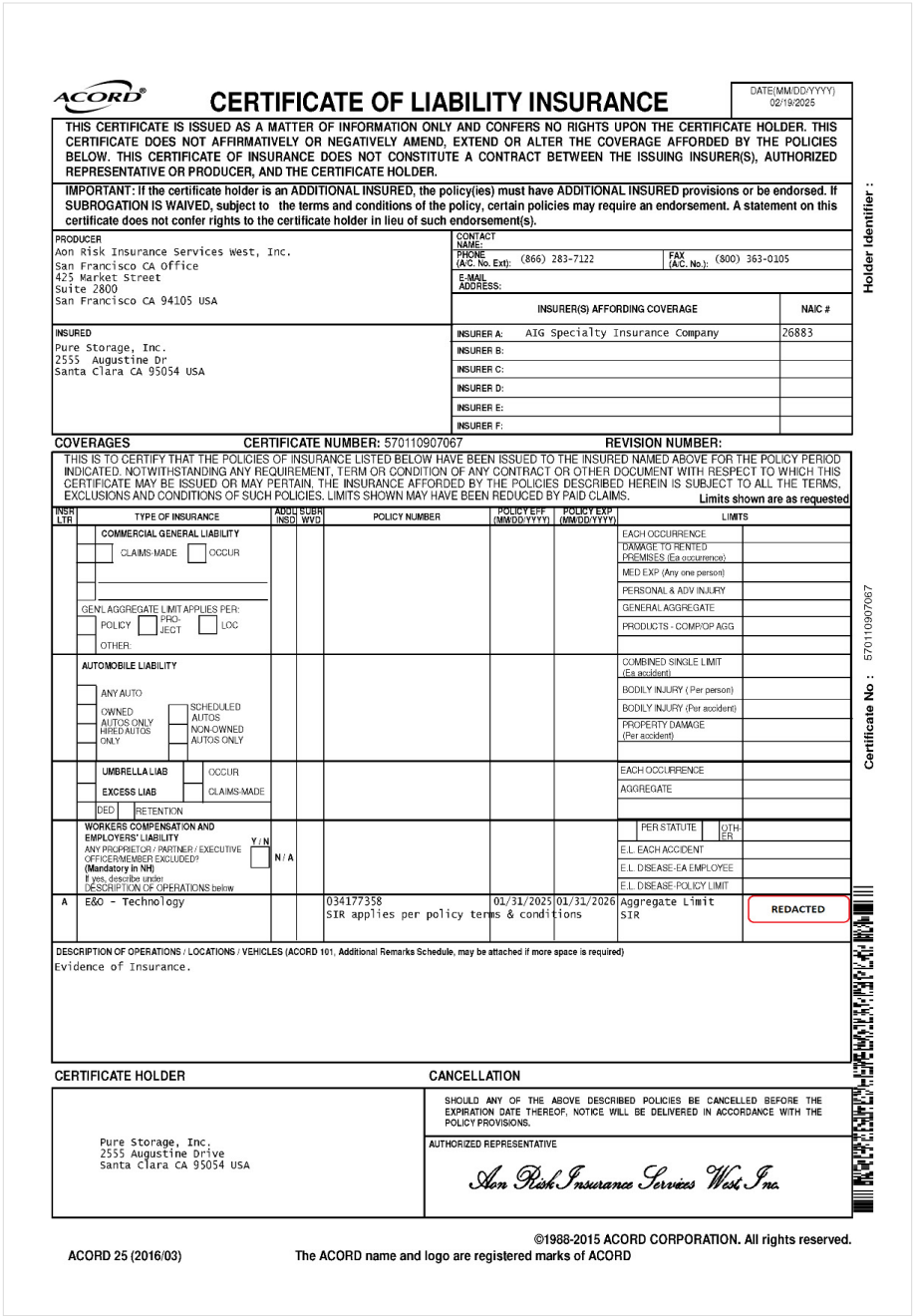
1. Software Producer Information
Company Name: Pure Storage, Inc.
Address: 2555 Augustine Drive
City: Santa Clara

[4] Attestations are binding for future versions of the named software product unless and until the software producer notifies the agencies to which it previously submitted the form that its development practices no longer conform to the required elements specified in the attestation.

5

Cyber Insurance Coverage

Pure Storage recognizes the critical importance of managing cybersecurity risks in today's digital landscape. To safeguard our operations, assets, and client data against the increasing prevalence of cyber threats, Pure Storage has implemented comprehensive cyber insurance coverage. This insurance plays a pivotal role in the company's broader risk management strategy, offering financial protection and support in the event of cyber incidents such as data breaches, cyber extortion, business interruption, and network damage. The cyber insurance policy for Pure Storage is tailored to address the specific risks associated with its operations in the tech industry, providing robust coverage that aligns with best practices and regulatory requirements. This proactive approach not only mitigates financial risks but also underscores Pure Storage's commitment to maintaining trust and reliability in its service delivery, ensuring that both the company and its clients are adequately protected in a landscape marked by evolving cyber threats.



ACORD®

CERTIFICATE OF LIABILITY INSURANCE

DATE(MM/DD/YYYY)
02/19/2025

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER
Aon Risk Insurance Services West, Inc.
San Francisco CA Office
425 Market Street
Suite 2800
San Francisco CA 94105 USA

CONTACT NAME:
PHONE (A/C, No, Ext): (866) 283-7122 FAX (A/C, No.): (800) 363-0105
E-MAIL ADDRESS:

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER A: AIG Specialty Insurance Company	26883
INSURER B:	
INSURER C:	
INSURER D:	
INSURER E:	
INSURER F:	

INSURED
Pure Storage, Inc.
2555 Augustine Dr
Santa Clara CA 95054 USA

COVERAGES CERTIFICATE NUMBER: 570110907067 REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS. Limits shown are as requested

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
	COMMERCIAL GENERAL LIABILITY CLAIMS-MADE OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: POLICY PRO-JECT LOC OTHER:						EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG
	AUTOMOBILE LIABILITY ANY AUTO OWNED AUTOS ONLY HIRED AUTOS ONLY SCHEDULED AUTOS NON-OWNED AUTOS ONLY						COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)
	UMBRELLA LIAB OCCUR EXCESS LIAB CLAIMS-MADE DED RETENTION						EACH OCCURRENCE AGGREGATE
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR / PARTNER / EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y / N N / A					PER STATUTE OTH-ER E.L. EACH ACCIDENT E.L. DISEASE-EA EMPLOYEE E.L. DISEASE-POLICY LIMIT
A	E&O - Technology			034177358 SIR applies per policy terms & conditions	01/31/2025	01/31/2026	Aggregate Limit SIR REDACTED

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
Evidence of Insurance.

CERTIFICATE HOLDER

Pure Storage, Inc.
2555 Augustine Drive
Santa Clara CA 95054 USA

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE
Aon Risk Insurance Services West, Inc.

Holder Identifier :
Certificate No : 570110907067

ACORD 25 (2016/03) The ACORD name and logo are registered marks of ACORD

Get in Touch

Resources and Contact Information

If you have any questions about our security practices or need more information, please reach out to your Account Management (AM) Team. If you don't know who your AM Team is, please contact Pure Storage Customer Support at support@purestorage.com or call us on +1-650-729-4088 and we will have your request routed properly.

For product-specific reports, such as concerns or issues related to vulnerabilities directly tied to Pure Storage products, please notify psirt@purestorage.com.

1 | This includes five years as a Leader in the Magic Quadrant for Solid-State Arrays and now six years as a Leader in the Magic Quadrant for Primary Storage.

PS2743-02-en 10/25