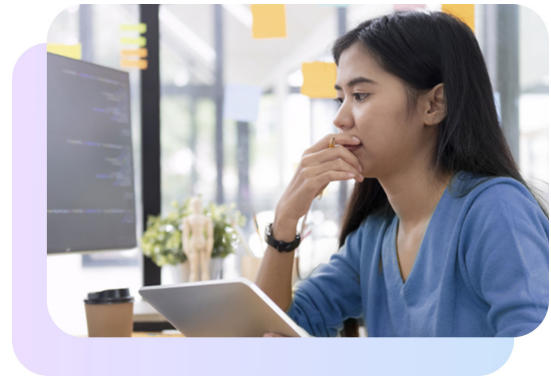






Protect your drive, protect your data

Data helps us innovate and create what's next for tomorrow. To help keep your data safe, Western Digital has a holistic security approach that covers all phases of a storage device's lifecycle: development, manufacturing, deployment, and use.


This paper describes Western Digital's security approach to data center and enterprise HDDs and SSDs, as well as smart video and NAS HDDs. These drives are protected by integrating security into the firmware, hardware, and manufacturing processes. We enable customers to protect their data by using encryption and access control.



Protect Your Drive

-  **Secure Manufacturing**
-  **Secure Boot**
-  **Secure Download**
-  **Secure Diagnostic**

Protect Your Data

-  **Encryption**
-  **Access Control**
-  **Data Sanitization**

Security Objectives

Western Digital's security approach is designed to achieve the following objectives:

- Help ensure that the drive is protected from outside interference during the manufacturing process
- Help ensure that the drive is protected against unwanted intrusion via third-party attack that could corrupt or alter drive functionality
- Help ensure that the user has tools to protect their data in the case of drive loss, physical access by a third party, or when a drive is removed from service

Western Digital's security architecture is based on a secure enclave to ensure that the drive is protected from cradle to grave from unwanted intrusion. A secure enclave is a dedicated secure subsystem that provides hardware-level isolation between security functionality and the remaining product functionality.

The secure enclave provides multiple cryptographic algorithm accelerators. Immutable code executes initialization, power-on self-test, and establishes root-of-trust. Secure enclave ensures device security lifecycle management, debug port management, asymmetric and symmetric root key management to bind key trees uniquely to the device. All cleartext key access is limited to the secure enclave.

Western Digital security features include

Hardware: Dedicated security hardware on each drive

Firmware: Dedicated security firmware implementation

Process: Secure manufacturing and diagnostic processes

Encryption: Support for industry standard encryption protocols

Access Control: Industry standard protocols to prevent unauthorized access to device



Protect Your Drive

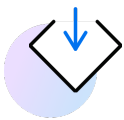
Western Digital security encompasses several steps throughout drive design and manufacturing. Security safeguards encompass customer shipment and deployment. In addition to internal validation of our security implementation, Western Digital engages third-party audits of various storage device integrity and data at rest protection claims. These third-party audits help confirm that our architecture reflects sound development practices, with strong supporting documentation and implementation.



Secure Manufacturing: These Western Digital drives are manufactured in trusted facilities with various secure manufacturing features and protections. Commands to securely manufacture the drive are authenticated by an in-house Certificate Authority (CA) Server and utilize security qualities to limit these commands to a specific drive serial number and one-time use. This functionality is only available within the Western Digital facility.



Secure Boot: The secure boot feature ensures that on every boot-up a drive verifies the firmware is from an authenticated source before it is used. The drive implements a multi-stage loader system during the boot process. Each loader stage is responsible for loading and verifying the next image before transferring control to the next image. This establishes a chain-of-trust during the boot process. The secure enclave is used to establish root-of-trust and enable the chain-of-trust.



Secure Download: The secure download feature ensures that only Western Digital signed firmware is accepted by a drive. A digital signature algorithm is used to verify the firmware signatures. To guarantee cryptographic separation, unique keys are used for different customers and security models. Additionally, Secure Rollback Prevention and Key Revocation features are made available.



Secure Diagnostics: When these drives ship from our factory all physical and logical debug ports are disabled. Commands to enable any debug capability on the drive are authenticated by the CA Server and utilize qualities to limit these commands to a specific drive identity (serial number) and one-time use. There are documented field failure analysis capabilities that utilize the same authentication mechanism.

Protect Your Data

To ensure confidentiality and integrity of the user data, there are three critical elements working in tandem. These features protect against the user data being accessed by unauthorized parties, either for read (confidentiality) or for write (integrity).



Encryption: Western Digital offers drives both with and without user data hardware-based encryption functionality. Drives with enabled encryption use AES-XTS-256 to encrypt user data at rest.



Access Control: Western Digital drives are available with industry-standard access control methods in both encrypted and non-encrypted drive models.



Data Sanitization: Drives of all interfaces (SATA, SAS, NVMe™) offer sanitize features that, when used properly, are consistent with the “Purge” functionality described by the IEEE Standard 2883™-2022 document, “Standard for Sanitizing Storage”.

Drive Type	Data Encrypted at Rest	Data Access Control	Preferred Purge-Erase	Certification
SE	No	ATA Security (SATA only)	Sanitize Overwrite (HDD) Sanitize Block Erase (SSD)	N/A
ISE	Yes	ATA Security (SATA only)	Crypto Erase	N/A
TCG	Yes	TCG-SSC	Crypto Erase Revert	No
TCG-FIPS	Yes	TCG-SSC	Crypto Erase Revert	FIPS 140-2 validation by NIST-approved labs (FIPS 140-3 in progress)

Summary

Securing data in today's environment requires multiple layers of protection. Western Digital integrates security into the firmware, hardware, and manufacturing processes to help ensure the physical drive is protected.

By enabling industry standard data encryption protocols and data access control we enable customers to protect their data. Western Digital's commitment to security and helping our customers secure what they create is at the heart of our products.

Learn more about Western Digital security solutions

www.westerndigital.com/solutions/data-security



Offered security types:

Secure Erase (SE): SE drives are offered without user-data encryption. User-data access control is provided, using the standard ATA Security feature set (SATA drives). Drive sanitization is performed using standard ATA Security Erase, SCSI Sanitize, or NVMe Sanitize commands, and incorporate the Overwrite (HDD) or Block Erase (SSD) methods.

Instant Secure Erase (ISE): ISE drives have data encrypted at rest. Access control is provided using the standard ATA Security feature set (SATA drives). The advantage of data encryption being enabled comes during the sanitization step. Drives can be sanitized using ATA, SCSI, or NVMe standard commands but with an instant cryptographic erasure rather than requiring that the drives be overwritten or go through a block erase process. Overwrite/block erase is also supported.

Trusted Computing Group (TCG): TCG drives have data encrypted at rest. Access control is handled through TCG-SSC protocols: TCG Enterprise, TCG Opal, or TCG Ruby depending on model. Drive sanitization can be done instantly using the Revert command. Cryptographic erase and overwrite/block erase is also supported.

TCG-FIPS: TCG-FIPS drives are functionally identical to TCG drives, but are validated by a NIST-approved laboratory to meet the United States Federal Information Processing Standard [FIPS]. In addition, drives use tamper-evident features to ensure that the drives are not physically modified during deployment or use.

