Micron SSDs: A secure foundation for your data[1]

IT managers, chief information officers (CIOs) and chief information security officers (CISOs) face ever-increasing threats from attackers attempting to illicitly acquire sensitive and valuable data. These threats call for a layered approach to data protection that addresses active data, as well as stored data.

Micron® SSDs help provide a secure defense for the base layer of your data systems. Data-at-rest protection covers data stored at various locations throughout the enterprise — from the notebook to the data center and in the cloud. Micron delivers SSDs for all these applications, built with advanced security technology, to help shield data from loss and to protect the security and integrity of the SSD and its firmware.

Threats to data at rest

Self-encrypting drives (SEDs) are widely recommended as the foundation to provide advanced protection against some of the most prevalent and dangerous threats to data at rest, including:

- **Lost or stolen computers or storage devices**: When powered off or in hibernation mode, SEDs automatically lock, inhibiting access to all data stored on the drive and requiring a passcode entry before being unlocked, decrypted and used.[2] Extremely robust 256-bit encryption means that the data is essentially unreadable without proper credentials.[3]
- **Sophisticated HDD/SSD attacks**: Sophisticated hackers have devised ways to attack HDDs and SSDs at their most basic level — the firmware. Micron SSDs, whether encrypted or not, include advanced protection features to ensure the authenticity of the firmware. Micron SSDs allow firmware updates in the field while significantly reducing the risk of loading a corrupted or counterfeited firmware image.[4]

Benefits of Micron self-encrypting drives (SEDs)

Encryption that does not slow you down

Built-in encryption engines perform at full interface speed, without using CPU cycles. Encrypted SSDs transfer data at the same speed as their unencrypted counterparts.[5]

Broad range of security options

Micron designs our SSDs with robust encryption and authentication features, as well as industry-standard data sanitization methods. Micron's encrypted SSDs meet multiple industry standards for security. Some Micron NVMe™ SSDs are also available with Micron's Secure Execution Environment (SEE).[6]

Security for the entire lifecycle of the device

- **Simplified key management**: The SSD generates and securely stores the encryption keys, removing that function from the host computer or data center.
- **Fast and secure device retirement/redeployment**: The cryptographic erase function securely sanitizes all user data in seconds, eliminating the need for costly and slow sanitation methods and enabling redeployment instead of wasteful device destruction.

[1] No hardware, software or system can provide absolute security under all conditions. Micron assumes no liability for lost, stolen or corrupted data arising from the use of any Micron products, including those products that incorporate any of the mentioned security features. SED behavior noted by the Storage Networking Industry Association (SNIA) in "Self-Encrypting Drives.".

[2] See: https://www.snia.org/sites/default/education/tutorials/2009/fall/security/MichaelWillett-Self_Encrypting_Drives-FINAL.pdf

[3] Estimate only, actual value may vary. Statement based on data from https://www.thesslstore.com/blog/what-is-256-bit-encryption/.

[4] One example of a firmware attack is noted here (this is just an example): https://usa.kaspersky.com/blog/equation-hdd-malware/5143/.

[5] Comparisons based on Micron testing with standard benchmarks on SED and non-SED SSDs (same model number and capacity).

[6] Statement based on SSD product briefs available at www.micron.com/ssd; the SEE is a dedicated security processing hardware with physical isolation for security-related function isolation built into specific SSD controller.

Micron SSD portfolio security features[7]

Table 1 shows security-related features and functions of Micron client and data center SSDs. When the feature or function is supported, a checkmark appears in the corresponding cell.

Feature / Micron SSD	Micron Client SSDs				Micron Data Center SSDs					
	2500	2550	2650	3500	5400	6500 ION	7450	7500	9550	XTR
Self-encrypted drive (SED)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cryptographic erase	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sanitize	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Secure erase	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
NAND block erase	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Signed firmware	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
TCG Enterprise					✓					
TCG Opal	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
TCG Pyrite	✓	✓	✓	✓						
TAA-compliant options					✓	✓	✓	✓	✓	✓
Micron Secure Execution Environment (SEE)						✓	✓	✓	✓	✓
Security Protocol and Data Model (SPDM)						✓	✓	✓	✓	✓
Ability to debug SSD without exposing user data						✓	✓	✓	✓	✓
FIPS certifiable (certification may not yet be complete)						✓	✓	✓	✓	✓
Attestation						✓	✓	✓	✓	✓
Secure boot	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Security engine: AES 256	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Security engine: RSA 4096	✓	✓	✓			✓	✓	✓	✓	✓
Security engine: SHA-512						✓	✓	✓	✓	✓

Table 1: Security-related features

Feature-rich Micron self-encrypting SSDs[7]

Micron secure firmware helps protect the storage platform against low-level attacks. Features like Advanced Encryption Standard (AES) 256-bit hardware encryption and standards-based security features work together to help protect your data (Micron is a contributing member of the Trusted Computing Group).[8]

Feature	Description
Self-encrypted drive (SED)	Self-encrypting drive; an SSD with an internal encryption mechanism or mechanisms.
Cryptographic erase	The process of erasing an SED by permanently destroying the encryption key.
Sanitize	A process by which data is removed from the storage device to a point that exceeds the ability to reconstruct the data by known forensic means.
Secure erase	Executing a block erase on each element in the NAND flash array in the SSD.
NAND block erase	The process of erasing an SSD via the NAND block erase command.
Signed firmware	Authenticates SSD firmware prior to updating it, which helps protect our SSDs against malicious firmware.
TCG Enterprise[9]	The Trusted Computing Group Enterprise standard is designed to provide more advanced security than Pyrite. The Opal standard can be used to encrypt user data in self-encrypting drives (SEDs). See https://trustedcomputinggroup.org/ for additional details.

Table 2: Security feature details

[7] Additional details on security features are available at: https://media-www.micron.com/-/media/client/global/documents/products/technical-marketing-brief/micron_ssd_security_features_tech_brief.pdf?la=en&rev=f33c44803f87439482348e38fcac6a58.

[8] Contributing members list available from https://trustedcomputinggroup.org/membership/member-companies/

[9] TCG Enterprise specification details: https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage-SSC_Enterprise-v1.01_r1.00.pdf

Feature	Description
TCG Opal[10]	The Trusted Computing Group Opal standard is designed to provide security by encryption user data on the SED. TCG Opal can help protect user data against unauthorized access. See https://trustedcomputinggroup.org/ for additional details.
TCG Pyrite[11]	The Trusted Computing Group Pyrite standard provides basic security but does not support user data encryption. See https://trustedcomputinggroup.org/ for additional details.
TAA-compliant options[12]	A standard providing assurance that Micron SSDs designated as TAA compliant are manufactured in TAA-designated countries to ease supply chain management for government users.
Micron Secure Execution Environment (SEE)	A dedicated security processing unit in select Micron SSD controllers. The SEE consists of a dedicated ROM, firmware, and security microprocessor. The secure microprocessor is electrically isolated from other microprocessors within the SSD controller; SEE execution cannot be preempted by non-secure code. This isolation significantly reduces the opportunity for the security functionality of the storage device to be accidentally or maliciously circumvented.
Security Protocol and Data Model (SPDM)	A standard that defines messages, data objects, and sequences for performing message exchanges between devices over a variety of transport and physical media. See The SPDM Protocol: Overview of Component Integrity as a Security Standard for additional details
Tamper-evident seals	Seals or labels encapsulating material or that provide evidence tampering.
Ability to debug SSD without exposing user data	The ability to troubleshoot SSD issues without having access to the user data on that SSD.
FIPS capable (but may not be certified)	A device that is capable of being certified to comply with the U.S. government FIPS specifications.
Attestation	A secure mechanism to validate trust in server components such as SSDs.
Secure boot	Utilizes a trust relationship between different entities where each entity honors the other’s authenticity, and each step is subject to attestation prior to execution (such as during power on). Micron SSD secure boot utilizes a chain of trust mechanism in which the SSD firmware bootloader trusts the immutable SSD ROM, and the main firmware in turn trusts the bootloader.
Security engine: AES 256	An open, standard encryption mechanism utilizing a 256-bit block.
Security engine: RSA 4096	A 4096-bit public key encryption mechanism based on an algorithm publicly disclosed in 1977.
Security engine: SHA-512	A one-way (hash) function that generates a 512-bit message digest.

Table 2: Security feature details (continued)

[10] TCG Opal specification details are available on the Trusted Computing Group website: https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage-Opalite_SSC_v1.00_r1.00.pdf

[11] TCG Pyrite specification details are available at the Trusted Computing Group website: https://trustedcomputinggroup.org/resource/tcg-storage-security-subsystem-class-pyrite/

[12] TAA-compliant devices available; contact your Micron sales team for additional information. Statement based on SSD product briefs available at www.micron.com/ssd

micron.com/ssd