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 your 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 the 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 come up with 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. They allow firmware updates in the field while significantly reducing the risk of loading a corrupted or counterfeited firmware image.[4]

BENEFITS OF MICRON SEDs

Encryption That Doesn't 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'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]

Micron SSD		Self-Encrypted (SED)	Crypto-graphic Erase	NAND Block Erase	Digitally Signed Firmware	TCG Enterprise[8]	TCG Opal[8]	TCG Pyrite[8]	TAA-Compliant Options[9]	Micron SEE
Client	2450	✓	✓	✓	✓		✓	✓		
	2550	✓	✓	✓	✓		✓	✓		
	3400	✓	✓	✓	✓		✓	✓		
Data Center	5400	✓	✓	✓	✓	✓	✓		✓	
	6500 ION	✓	✓	✓	✓		✓		✓	✓
	7450	✓	✓	✓	✓		✓		✓	✓
	9400	✓	✓	✓	✓					
	XTR	✓	✓	✓	✓		✓		✓	✓

Feature-Rich Micron Self-Encrypting SSDs

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
SED	Self-encrypting drive, an SSD with an internal encryption mechanism or mechanisms.
Cryptographic Erase	The process of erasing an SED by removing the encryption key.
NAND Block Erase	The process of erasing an SSD via the NAND block erase command (sets all NAND cells to the same value, typically a 1).
Digitally Signed Firmware	Mechanism to verify the authenticity of the firmware.
TCG Enterprise[10]	The Trusted Computing Group Enterprise standard is designed to provide security for storage devices deployed in data centers to help protect against data loss due to physical storage device theft.
TCG Opal[11]	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.
TCG Pyrite[12]	The Trusted Computing Group Pyrite standard is designed to provide basic security without data encryption.
TAA Compliant	A standard providing assurance that Micron SSDs designated as TAA compliant are manufactured in TAA-designated countries and easing supply chain management for government accounts.
Micron SEE	A dedicated security processing unit in specific Micron SSD controllers (not present in all SSDs).

Security feature details

7. Additional details on security features is available here: 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. TAA-compliant devices available; contact your Micron sales team for additional information. Statement based on SSD product briefs available at www.micron.com/ssd
10. TCG Enterprise specification details are available at the Trusted Computing Group website: https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage-SSC_Enterprise-v1.01_r1.00.pdf
11. 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
12. TCG Pyrite specification details are available at the Trusted Computing Group website: https://trustedcomputinggroup.org/resource/tcg-storage-security-subsystem-class-pyrite/

micron.com/ssd