EXASCEND

SECURITY

Fortify your security with Exascend AES-256 & TCG Opal 2.0

EXASCEND SECURE SSDs

Exascend's self-encrypting drives (SEDs) are fully compliant with the TCG Opal 2.0 specifications and utilize AES-256 encryption to provide customers with the highest level of security. Fully customizable and equipped with powerful patented technologies, Exascend's SEDs are perfect for any application that demands highly secure high-quality storage.

FEATURES

Self-encrypting drive (SED)

Self-encrypting drives store all data in encrypted format, making it impossible for malicious actors to simply steal a storage device to access the data stored within. In SEDs, data is scrambled at the hardware level, thus improving data security with only a negligible impact on performance.

AES-256

The Advanced Encryption Standard (AES) is a U.S. encryption specification used for securing sensitive data, including the highest level of classified information, i.e., Top Secret. AES-256 uses the highest-security 256-bit key size, providing virtually impenetrable security.

TCG Opal 2.0

TCG Opal 2.0 is a set of specifications for SEDs established by the Trusted Computing Group (TCG), a consortium of leading technology companies. Compliance with the TCG Opal 2.0 specifications protects user data from unauthorized access and guarantees industry-wide device interoperability.

Complete data sanitization

Exascend's secure SSDs offer three types of data sanitization to meet all security requirements. Fast erase deletes the mapping table, rendering data useless in under a second. Normal erase deletes the mapping table and all data, making recovery completely impossible. Cryptographic erase deletes the mapping table and changes the encryption key, sanitizing all data in the process.

BENEFITS

Perfect for the edge

Edge and IoT devices are uniquely exposed to external security threats. Exascend's secure SSDs ensures that data is safe even in the event of device theft.

High interoperability

TCG Opal 2.0 enables compatibility across devices and operating systems, guaranteeing that fortified security is possible in any system and operating environment.

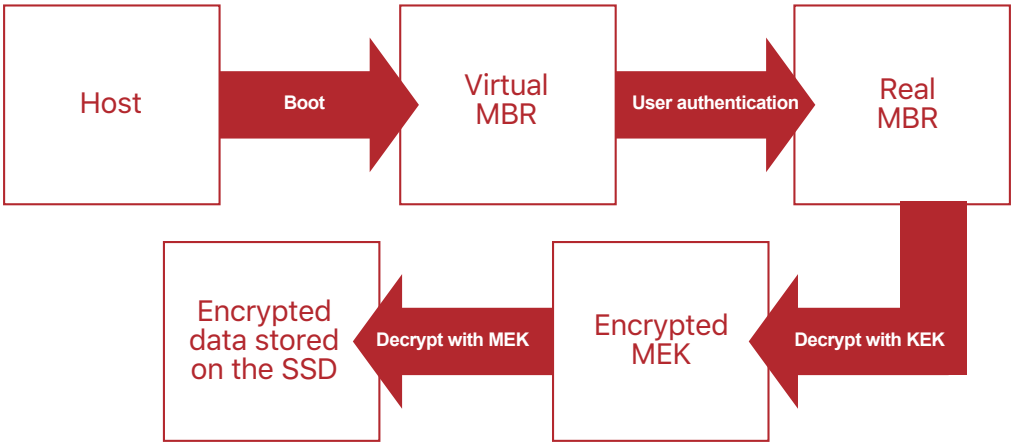
Unbeatable security

The combination of the impenetrable AES cipher and hardware encryption provides data security invulnerable to software and operating system-level breaches.

Blazing-fast

Hardware encryption ensures that the task of encrypting and decrypting data is left to the storage device instead of wasting valuable system resources.

HOW DOES IT WORK?



1. Upon boot, the system accesses the virtual master boot record (MBR) where the user has to enter their password.
2. Once the correct password has been entered, the real MBR decrypts the media encryption key (MEK) with the now-unlocked key encryption key (KEK).
3. The MEK is used to encrypt and decrypt data stored on the SSD, allowing seamless data read/write.
4. As soon as the system loses power, re-authentication is required to access the AES-encrypted data.

RECOMMENDED APPLICATIONS

- **Mission critical**
- **Edge computing**
- **Telecommunications**
- **Transportation**

RECOMMENDED PRODUCTS

PE3

- AES-256 encryption
- TCG Opal 2.0-compliant
- PCIe 3.0 (NVMe 1.2) interface
- 3D TLC NAND flash
- Up to 8 TB capacity
- 3,100 MB/s sustained read
- 2,000 MB/s sustained write

SE3

- AES-256 encryption
- TCG Opal 2.0-compliant
- SATA-III interface
- 3D TLC NAND flash
- Up to 4 TB capacity
- 530 MB/s sustained read
- 535 MB/s sustained write