M.2 SSD

- **M.2 Secure SED**

Reliable hardware level self-encrypting high performance SSD drives support a wide range of SSD applications.

- **M.2 SATA - TCG Opal 2.0**
  - ✓ 256GB
  - ✓ 512GB
  - ✓ 1TB
  - ✓ 2TB

- **M.2 PCIe Gen 3x4 NVMe - TCG Opal 2.0**
  - ✓ 256GB
  - ✓ 512GB
  - ✓ 1TB
  - ✓ 2TB
  - ✓ 4TB

1) TCG Opal Pre-boot authentication: Authenticating access before the computer boots protects the integrity of the OS.
2) Advanced Encryption: Built-in Advanced Encryption Standard (AES) 256-bit hardware encryption engine.
3) TAA Compliant

M.2 SSD Secure SED are Self-Encrypting Drives securing all critical data using strong AES 256-bit Encryption. TCG Opal 2.0 hardware level AES 256-bit encryption means the encryption/decryption is performed on device, independent from the host, reducing CPU load.

- **M.2 SATA - FIPS 140-2**
  - ✓ 128GB
  - ✓ 256GB
  - ✓ 512GB
  - ✓ 1TB
  - ✓ 2TB

- **M.2 PCIe Gen 3x4 NVMe - FIPS 140-2**
  - ✓ 256GB
  - ✓ 512GB
  - ✓ 1TB
  - ✓ 2TB

1) FIPS 140-2 certified: The internal flash build has been Independently certified by one of 13 NIST specified laboratories examining the cryptographic modules. Certified by NIST's Cryptographic Module Validation Program (CMVP). For more information, refer to the NIST site.
2) NIAP-listed Common Criteria (CC) SSD for Full Drive Encryption – Encryption Engine Common Criteria (CC) collaborative Protection Profile (cPP)
3) Secure Firmware: Solid secure firmware features secure digital signatures and boot-time attestation which help to protect storage devices against low-level attacks.
4) Hardware level AES 256-bit encryption with TCG Opal SSC support: the encryption/decryption is performed on device, independent from the host, reducing CPU load.
5) Instant Erase: The ability to complete sanitization of all data on the SSD in under 2 seconds, simplifying device retirement or redeployment.
6) Conformal Coating as tamper evidence on board for physical security.
7) Our Citadel SEDs make use of the TCG Opal Pre-boot authentication support to authenticate access before the computer boots, which protects the integrity of the OS.
8) 3rd party key management options include but not limited to are: Absolute Software, CryptoMill, McAfee, Secude, Softex, Sophos, Symantec, Wave Systems and WinMagic. Linux FDE (Full Disk Encryption) key management methods also supported.
9) TAA Compliant

FIPS 140-2 L2

Secure SED FIPS 140-2 L2 M.2 SATA SSD drives are self-encrypting drives securing all critical data using strong AES 256-bit encryption. FIPS 140-2 Level 2 hardware encryption ensures that the firmware integrity, encryption technology and physical security of the SSD all meet the requirements set forth by the Federal Information Processing Standard by the National Institute of Standards & Technology (NIST).

NIAP-Listed, TAA Compliant, and Common Criteria Certified

All Citadel K-Series SEDs are NIAP-compliant (VID #11297), TAA compliant, and have been listed by NIST as FIPS 140-2 L2 certified storage devices with NIST Certificate #3926, ensuring they meet most stringent cybersecurity standards.

Commercial Solutions for Classified

DIGISTOR's FIPS SEDs are listed on the NSA CSfC Component List for hardware full drive encryption, which allows DoD, Federal agencies, and critical infrastructure to protect mission critical and classified data using commercial solutions.