

Software Full Drive Encryption Data Sheet

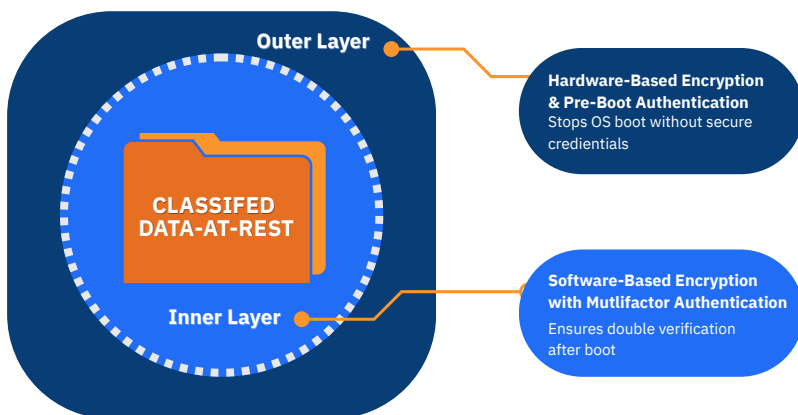
NSA CSfC-Compliant Inner Layer Protection

Cigent Software Full Drive Encryption (FDE) secures mission-critical data and delivers the inner layer encryption required under the NSA's CSfC Data at Rest (CSfC DAR) capability package. Designed to meet strict federal compliance standards, Cigent Software FDE employs quantum-resistant AES 256-bit encryption.

The solution complements hardware full drive encryption and Pre-Boot Authentication (PBA) to provide a single solution to meet CSfC DAR guidelines. Cigent Software FDE can also be deployed as a standalone solution to provide secure software-based encryption for protecting sensitive data at rest in environments that do not require a full CSfC implementation.

Cigent Software FDE is an essential safeguard for classified and sensitive information against unauthorized access and data breaches.

CSfC for DAR Protection



Cigent Software FDE employs independent and distinct cryptographic libraries from Cigent Hardware FDE to meet the NSA's CSfC Data at Rest (DAR) manufacturer diversity requirement. This allows Cigent to provide both the inner and outer layers of a complete CSfC DAR-compliant solution.

Key Features:

- **NSA CSfC Compliant:** Provides the mandated inner layer encryption for CSfC DAR compliance, ensuring alignment with NSA requirements to protect classified and sensitive data.
- **Pre-OS Authorization:** Cigent employs pre-OS boot requiring users to authenticate before the operating system boots. The approach reduces the risk of the OS being compromised to gain access to keys.
- **Multi-factor Authentication:** Ensures that only authorized users can access encrypted data by requiring the use of both username/password and a smartcard (CAC).
- **Administration at Scale:** Command line interface provides management of SW FDE with ability to integrate into existing enterprise management.
- **Extensive Device Coverage:** Supports PCs, mobile workstations, and servers running Windows or Linux. SW FDE can also be employed on non-traditional compute devices including vehicles, UxV, and ICS.

Cigent SW FDE can also be utilized with other suppliers' CSfC compliant drives to provide the inner layer of CSfC DAR protection requirements.

How Cigent FDE Secures Your Data

Cigent Software Full Drive Encryption safeguards sensitive data from power-off through system boot, aligning with the NSA CSfC DAR capability package requirements for the inner encryption layer. This layer operates independently of the hardware and protects data at rest with strong cryptographic controls and multi-factor authentication.

1. **Power-Off Protection:** When the device is powered off, all data on the drive remains encrypted and unreadable.
2. **Boot-Time Enforcement:** Upon power-on, the SW FDE requires authentication before the operating system loads, enforcing access control before any data is decrypted.
3. **Two-Factor Access Control:** Access to encrypted data requires authentication using both a username/password and a smartcard (CAC).
4. **Transparent Data Access:** Once authenticated, the encryption engine fully decrypts the drive, allowing users to seamlessly access their data without friction.

A Complete CSfC for DAR Solution

Cigent FDE can be deployed alongside Cigent's hardware full drive encryption (HW FDE) and Pre-Boot Authentication (PBA) as complementary, independently operating solutions to deliver both the inner and outer layers required by the NSA's CSfC Data at Rest (DAR) Capability Package. This combination forms a complete solution for meeting CSfC's dual-layer encryption mandate.

Each layer operates independently, with no crossover in cryptographic libraries or functional roles, ensuring full compliance with CSfC architectural separation requirements. The result is a highly flexible deployment model that reduces complexity while assuring compliance.

By sourcing both layers from Cigent, organizations can simplify procurement, accelerate deployment, and ensure compatibility, all while meeting the most stringent security standards set by the NSA.

Schedule a Demo

See how Cigent keeps you AlwaysPROTECTED.

[Book a Demo](#)

www.cigent.com

info@cigent.com

844.256.1825