CSfC for Data at Rest Protection

As data at the edge is highly vulnerable to compromise, the NSA established the Commercial Solutions for Classified (CSfC) program setting minimum requirements to protect classified data at rest (DAR) on endpoints. The NSA mandates a layered approach requiring a combination of hardware encryption and pre-boot authentication (PBA). Cigent enables you to meet CSfC for DAR compliance, ensuring the integrity of your data for PCs and Servers

Benefits of CSfC for DAR

AES-256 Full Drive Hardware Encryption with PBA

Full drive hardware encryption is the foundation for protecting data on endpoints. Cigent encryptions uses proven methodology and technology ensures keys are inaccessible to advanced threat actors. Supporting NSA's "layered" approach Cigent"...complement hardware encryption with pre-boot authentication that certifies credentials before the system can boot the drive. Optional multi-factor authentication (MFA) is also supported requiring a combination of password and smart card."

Supporting Ecosystem

Mission success requires teamwork, and data protection is no different. Cigent proactively works with a rich ecosystem of partners to streamline acquisition, deployment, and utilization of secured storage. Secured storage is available directly from major device manufacturers, including Dell and HP. In addition, all major CSfC SIs have validated and are utilizing the Cigent data protection solution.

Protection Capabilities

To ensure the integrity of sensitive data, Cigent complements hardware encryption with unique, patented data protection capabilities.

Enterprise Administration

Cigent provides an enterprise management console that can be deployed in the cloud or on premises and a Command Line Interface (CLI) supporting key management, compliance reporting, policy setting, and deployment automation.

Cloning and Wiping Prevention

Full drive encryption and hidden partitions lock all ranges preventing malicious compromise. Data secured within hidden partitions remain unreadable even if the device is in use.

Data Erasure

Data can be erased through a local or remote command utilizing crypto and full block erase. Provides emergency data erasure and can enable drive reuse.

Secure Command Logs

All data activity is recorded in secure, tamper-proof logs. Prevents malicious actors from "covering their tracks" with irrefutable documentation of activities.

Committed to Your Mission's Success

Cigent provides unparalleled technology, ecosystem, and expertise to ensure your sensitive data is protected no matter what your mission. The Cigent solution was developed for and with US Federal agencies by leading experts in data recovery and sanitization. Cigent is a trusted partner in addressing your data protection at the edge requirements. We will work with you to understand your mission requirements and ensure you have data protection that will enable your success.

Book a demo today!