CIGENT
AlwaysPROTECTED™

PROTECT DATA AT THE EDGE
Protecting your data, enabling your mission

PCs Secure Drive Data Sheet

PCs are critical productivity tools where sensitive data is processed and stored. To ensure the integrity of the data, it is essential that they use full drive hardware encryption with pre-boot authentication (PBA). Cigent Secure Storage has undergone rigorous testing to ensure data cannot be exfiltrated from compromised devices.

Cigent Secure Storage

AES 256-bit Hardware Encryption.

Cigent proven and tested methodology for encryption that has undergone rigorous testing by NSA, DISA, and other Federal agencies.

Pre-boot Authentication (PBA).

PBA is a critical security capability to prevent adversaries from circumventing full drive encryption. PBA provides a separate, secure authentication prior to initiating boot. Cigent PBA has been validated by the NSA for CSfC for DAR.

Multifactor Authentication (MFA).

Optional configuration with PBA provides MFA capability requiring use of both U/N Password and smart card (CAC).

Drive Portfolio

Ensuring protection is available for a variety of PCs Cigent with our partners offer 2280 and 2230 drives.

- **2280 Secure Storage:** 2280 is the legacy standard for storage configuration on PCs. Drive options include:
  - **Secure Drive 2280 CSfC SSD Bravo**. *NSA CSfC DAR Component List*. Key features include full drive hardware encryption with PBA, enterprise management, hidden partitions, cloning and wipe prevention, verified data erasure, and command logs.
  - **Secure Drive 2280 FIPs SSD Bravo**. *FIPS 140-2 Certified*. Key features include full drive hardware encryption with PBA, enterprise management, hidden partitions, cloning and wipe prevention, verified data erasure, and command logs.
  - **Secure Drive 2280 SSD Charlie.** Key features include full drive hardware encryption with PBA, enterprise management, hidden partitions, cloning and wipe prevention, crypto and full block erasure, command logs, *AI-secured storage*, and *verified data erasure.*

- **Secure Drive 2230 SSD Alpha.** Features include full drive hardware encryption with PBA, enterprise management, hidden partitions, cloning and wipe prevention, data erasure, and crypto and full block erasure.

The Secure Drive 2230 utilizes the same architecture as 2280, including the NSA-approved PBA.
2230 is an emerging standard for device manufacturers' storage configurations, including Microsoft Surface, Dell Latitude, and HP EliteBooks.

Features

Encryption and PBA provide foundational data security, but evolving sophisticated adversaries present additional risk. Cigent provides a portfolio of cyber security features to mitigate risk. These include:

- **Administration:** Beyond the encryption of data, organizations also are required to address other requirements including recovering and destroying data on returned systems, incident response, and policy reporting. For key management, compliance reporting, policy setting, and deployment automation, Cigent provides an enterprise management console that can be deployed in the cloud or on premises and a Command Line Interface (CLI) tool that runs in Linux and Windows.

- **Hidden Partitions:** All Cigent Secure Storage provides the option to create hidden partition generating enclaves to store sensitive data preventing an adversary from discovering even the existence of the data. The hidden partitions are unreadable at the sector level even after logging onto the device until unlocked using step-up authentication.

- **Cloning and Wiping Prevention:** All Cigent Secure Storage protects against illicit wiping and cloning. Data at rest protection is protected with full drive hardware encryption that locks all ranges. Cigent is unique in also preventing cloning when the device is in use through its ability to create hidden partitions. The hidden partitions also lock all ranges preventing wiping and cloning. These partitions also provide hidden environments to store sensitive data preventing an adversary from discovering even the existence of the data.

- **Verified Data Erasure: P**atented technology that ensures all data on a drive has been permanently deleted. Ability to locally or remotely execute a cleanse that erases all data via crypto and block erasure followed by block-by-block validation. Solution provides confidence in emergency data destruction situations, addresses risk from emerging quantum capabilities, and provides potential for drive reuse.

- **AI Secured Storage**: Only AI embedded in storage continually monitors data access patterns instantly securing data when anomalous behavior is detected. Detects if alternate O/S boot approach is attempted. AI is tamper proof providing continuous monitoring of sensitive data.

Cigent Advantages

Complementing Cigent unparalleled technical features is a robust ecosystem of device manufacturer and FSI partners. Cigent secure drives have been validated and utilized by leading FSI including Booz Allen, Allen Hamilton District Defend, AFRL's SecureView, Everfox Trusted Thin Client, Integrated Global Security, Army APG, and CACI ID Tec's Archon.

CIGENT AlwaysPROTECTED™

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