CIGENT
AlwaysPROTECTED™

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

2230 Cigent Secure Drive

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).

2230 is an emerging standard for device manufactures storage configurations including Microsoft Surface, Dell Latitude, and HP EliteBooks. Cigent is unique providing secure storage capabilities for 2230 including NSA-validated PBA.

Cigent Secure Storage 2230 Encryption and PBA

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).

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: A**ll 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.

Complementing Cigent unparalleled technical features is a robust ecosystem of device manufacturers and FSI partners. Cigent enabled secured storage can be purchased with PCs and Servers from device manufacturers including Dell, HP, and GETAC. In addition, Cigent secure drives have been validate 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