CIGENT
AlwaysPROTECTED™

SERVER | DATA SHEET

PROTECT DATA AT THE EDGE

PROTECTING YOUR DATA, ENABLING YOUR MISSION

Edge computing requirements are increasing the utilization of servers outside of secured data centers. Servers have become compact and lighter with an induvial server weighing as little as 25 pounds making them increasingly susceptible to theft. Additionally, as servers are likely to process and store even more data than PCs, it is imperative to ensure data is protected.

Cigent Secure Enterprise Storage, 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 adversary from circumventing full drive encryption. PBA provides a separate, secure authentication prior to initiating boot. Cigent PBA has been validated by 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 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.

- **Inaccessible Keys:** Cigent employs proven methodology and technology for the creation and storage of keys that renders all known compromises approaches obsolete. Keys are created using maximum characters allowed, deconstructed and distributed throughout the drive preventing even sophisticated adversaries from compromise.

- **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 Enterprise Storage protect 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.

- **Data Erasure:** all Cigent Secure Enterprise Storage enabled drives provide the ability to locally or remotely execute a cleanse that erases all data via crypto and block erasure.

- **Secure Logs:** select Cigent Secure Enterprise Storage include the capability to collect and securely store all data-related activity. The logs prevent a malicious actor from “covering their track.” Log activity can enable detection of malicious activity and can be used for incident response.

Schedule a Demo with Us to Learn More!

- **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.

Cigent offers a portfolio of secured storage options to meet mission requirements. This includes:

- **Secure Enterprise Storage 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.

- **Secure Enterprise Storage CSfC Alpha.** NSA CSfC DAR Component List. Features include full drive hardware encryption with PBA, enterprise management, hidden partitions, cloning and wipe prevention, data erasure, and crypto and full block erasure.

- **Secure Boot 2280 SSD Bravo.** A boot drive is a storage device that contains the files needed to start a computer's operating system (OS) or firmware when it is turned on or restarted. Cigent ensures these critical drives are protected with features including full drive hardware encryption with PBA, enterprise management, hidden partitions, cloning and wipe prevention, verified data erasure, and command logs.

Complementing Cigent unparalleled technical features is a robust ecosystem of device manufacturer 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 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 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.

Schedule a Demo with Us to Learn More!