Sourcing Secure Storage to Protect Sensitive Data at the Edge

CIGENT

Emerging technologies and evolving mission requirements are driving the rapid expansion of sensitive data at the edge. A growing portfolio of devices either are collecting, processing, and storing sensitive data. Cigent provides an unparalleled breadth of storage drives with hardware-based encryption enabling operators to achieve compliance mandates and ensure data remains protected in any environment. The extensive Cigent portfolio includes coverage for PCs, Servers, Tablets, Removable Media, and Embedded with multiple storage devices meeting automotive standards for use in manned and unmanned vehicles.

Cigent is prepared to support your mission navigating the complex compliance requirements to protect data at the edge. Its solutions were developed for and with US Federal agencies with deep expertise in data protection. Cigent protections have been thoroughly tested and validated by leading Federal agencies including MITRE, NIST, NSA, NIAP, the Air Force, Cyber Resilience of Weapon Systems (CROWS), and NSSIF (UK).

To ensure availability and provide flexibility, Cigent works with leading drive manufacturers including Digistor, Kanguru, and Seagate and Cigent offers our own branded drives.

This document is designed to help you identify the solutions for your specific mission requirements.

Cigent Features

Effective protection of data at rest (DAR) requires layers of protection technology to prevent unauthorized access. Cigent's solution uses proven, and NSA validated encryption methodology, including full drive AES-256-bit hardware encryption. This encryption is supplemented by pre-boot authentication (PBA) providing an additional outside layer of protection that certifies credentials before the system can boot the drive. The Cigent solution has been certified by the NSA and with drive partners is listed on the CSfC for DAR component list.

While DAR protection with full drive encryption is fundamental, Cigent complements its security with a patented portfolio of data protection features to ensure sensitive data remains secure in all aspects of an operation. These features streamline administration and reporting, provide additional protection for physical and remote threats, and address critical data hygiene challenges.

The Cigent portfolio of features includes:

Enterprise Management:

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 key that renders all known compromises approaches obsolete. Keys are created using maximum characters allowed, deconstructed and distributed throughout 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 Storage protect against illicit wiping and cloning. Data at rest protection is protected with full drive hardware encryption that lock 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 Storage enabled drives provide the ability to locally or remotely execute a cleanse that erases all data via crypto and block erasure. Selected drives also provide Verified Data Erasure, a patented solution that performs block-by-block analysis to ensure that all data has been permanently erased. Solution provides confidence in emergency data destruction situations, addresses risk from emerging quantum capabilities, and provides potential for drive reuse.

Secure Data Logs:

Multiple Cigent Secure Storage 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.

AI Secured Storage:

Selected Cigent Secure Storage include patented embedded AI protection. The AI monitors data access patterns instantly securing data when a threat is detected. AI monitoring can detect if an adversary is utilizing alternative OS boot.

Advanced Physical Detection:

For organizations with the highest secure requirements Cigent offers Secure Storage devices that include a combination of extended life, accelerometers, and physical tampering detection.

Cigent’s array of capabilities are organized by Feature Packages for its drive portfolio.

Alpha AES-256 Hardware Full Drive Encryption, Enterprise Management, Inaccessible Keys, Hidden Partitions, Cloning/Wiping Prevention, Crypto Wipe & full Block Erase

Bravo All Alpha capabilities + Verified Data Erasure Hidden Partitions Plus, Command Logs

Charlie All Bravo capabilities + AI Secured Storage including ransomware M/L detection and response and alt O/S boot prevention

Delta All Charlie capabilities + Capacitors maintain power after drive unplugged for up to two weeks, accelerometer, disconnect detection circuit

Cigent Drive Portfolio

Evolving technology and mission requirements is resulting in a proliferation of devices with sensitive data at the edge. Cigent provides the most extensive portfolio of secured storage devices providing a single trusted partner to ensure all endpoint data is protected.

The Cigent portfolio includes:

- PCs & Tablets
- Servers
- External Media
- Embedded Devices
- Unmanned Vehicles
- Custom solution

PCs and Tablets

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

Cigent Secure Storage have undergone rigorous testing to ensure data cannot be exfiltrated from compromised devices.

Ensuring protection is available for a variety of PCs Cigent with our partners offer 2230 and 2280 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 manufactures storage configurations including Microsoft Surface, Dell Latitude, and HP EliteBooks.

Servers

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. Like with PCs, the foundation of data protection is AES-256 encryption and PBA with optional MFA.

- **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.

External Media

External media includes a variety of storage devices including flash drives, external storage devices, and SD and MicroSD Cards. Advancement in storage capabilities enable these small form factors to store massive amounts of potentially sensitive data. Additionally, they are small and lightweight increasing the likelihood of loss from negligence or malicious actions.

- **Secure Flash Drive Alpha.** High performance, reliable meeting Industrial temperature specifications and able to store 64 GB of data. Features include full disk hardware encryption with PBA, enterprise management, hidden partitions, cloning and wipe prevention, data erasure, and crypto and full block erasure.
- **Secure External Encrypted Storage.** Providing a secure method to transport and store sensitive data, Cigent offers a portfolio of external encrypted storage devices to meet your security requirements. All devices are high performance with storage capacity of 2 or 4 TB.
  - **External Encrypted Storage FIPS SSD Bravo.** *FIPS 140-2 Certified.* Key features include full disk hardware encryption with PBA, enterprise management, hidden partitions, cloning and wipe prevention, verified data erasure, and command logs.
  - **External Encrypted Storage FIPS SSD Charlie.** Key features include full disk 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.

- **External Encrypted Storage FIPS SSD Delta.** Providing the most secure data storage available.

  Key features include full drive hardware encryption with PBA, enterprise management, cloning and wipe prevention, hidden partitions, crypto and full block erasure, command logs, AI secured storage, verified data erasure, and *advanced physical protection.*

  Advanced physical protection ensures integrity of device. Features include capacitors able to maintain power for two weeks, accelerometers detecting and recording any movement, and disconnect detection circuit that will automatically execute crypto and block wipes following unauthorized reconnect.

SD and MicroSD. With flash memory, these ubiquitous cards are used in an array of portable electronics including PCs, tablets, cameras, GPS devices, and unmanned vehicles. As they are often in demanding environments, the devices need to be rugged and meet industrial temperature requirements (-40 to 85 C).

Given their role supporting missions, a key feature will be the ability to remotely crypto and block erase data. Additionally, as they may be in immediate proximity with adversaries, Cigent unique ability to prevent cloning and wiping is invaluable.

- **Secure SD Encrypted Alpha.** Provides 64 GB of storage and meets industrial temperature standards. Features include hardware encryption, enterprise management, hidden partitions, cloning and wipe prevention, data erasure, and crypto and full block erasure.
- **Secure MicroSD Encrypted Alpha.** Provides 64 GB of storage and meets industrial temperature standards. Features include hardware encryption, enterprise management, hidden partitions, cloning and wipe prevention, data erasure, and crypto and full block erasure.

Embedded Devices

Embedded devices are flash memory with Ball Grid Array (BGA) for surface-mount packaging used for integrated circuits. These storage devices are intended to be embedded within a device.

SSD BGA Encrypted Alpha. Designed for use in manned and unmanned vehicles, provides 1 TB of storage and meets automotive temperature standards (-40 to 105 C). Features include hardware encryption, enterprise management, hidden partitions, cloning and wipe prevention, data erasure, and crypto and full block erasure.

Unmanned Vehicles

Unmanned vehicles have already established themselves as an essential element for military and civilian operations. Rapid improvements in their capabilities will accelerate adoption for a variety of tasks. Two types of data on unmanned vehicles need to be protected: 1.) proprietary algorithms on the device are of a highly sensitive nature and represent significant investments; 2.) data collected by the vehicle is also likely to be sensitive.

Unmanned vehicles will utilize a variety of storage devices including 2230 drives, SSD BGA, and SD and MicroSD cards. To ensure data integrity it is essential that all are using full drive hardware encryption. All Cigent storage provides AES-256 full drive hardware encryption with additional data protection to support unmanned vehicle operations. Key additional capabilities include:

- **Hidden Partitions:** All Cigent Secure Storage includes the capability to create hidden partitions to store sensitive data. Partitions lock all ranges to prevent wiping or cloning and prevent adversary from detecting the presence of data. As hidden partitions cannot be read at the sector level, they provide unmanned vehicle operators with a hidden environment to store their valuable algorithms.
- **Data Erasure:** Data can be safely erased with the ability to locally or remotely execute an erasure program. Data is crypto erased followed by block erasure. Capability provides operators with emergency data erasure and provides flexibility to reuse drives.

Cigent is unique in its ability to provide an array of protected storage designed to meet the rigorous environment of unmanned vehicles.

- **Secure Drive 2230 SSD Alpha.** Features include full 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.
- **Secure Drive SSD BGA Encrypted Alpha.** Meets automotive temperature standards (-40 to 105 C). Features include hardware encryption, enterprise management, hidden partitions, cloning and wipe prevention, data erasure, and crypto and full block erasure.
- **Secure Drive SD Encrypted Alpha.** Provides 64 GB of storage and meets industrial temperature standards. Features include hardware encryption, enterprise management, hidden partitions, cloning and wipe prevention, data erasure, and crypto and full block erasure.
- **MicroSD Encrypted Alpha.** Provides 64 GB of storage and meets industrial temperature standards. Features include hardware encryption, enterprise management, hidden partitions, cloning and wipe prevention, data erasure, and crypto and full block erasure.