CIGENT
AlwaysPROTECTED™

EXTERNAL MEDIA | DATA SHEET

PROTECT DATA AT THE EDGE

PROTECTING YOUR DATA, ENABLING YOUR MISSION

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.

Cigent provides a portfolio of Secure Storage options for remote media. All devices include foundational AES 256-bit Hardware Encryption. Cigent proven and tested methodology for encryption that has undergone rigorous testing by NSA, DISA and other Federal agencies. It provides foundational protection for data at rest.

Evolving sophisticated adversaries present additional risk. Cigent provides portfolio of cyber security features to mitigate risk specifically for remote media storage. These features 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.

- **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.

- **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 and Verified Data Erasure:** all Cigent Secure External Media Storage provide the ability to locally or remotely execute a cleanse that erases all data via crypto and block erasure. Select storage also includes that capability to verify all data has been permanently erased. Block by block analysis confirms data erasure and can re-execute erasure as required.

- **Secure Logs:** select Cigent Secure External Media 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.

- **AI Secured Storage:** selected all Cigent Secure External Media 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 employing 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.

Schedule a Demo with Us to Learn More!

Cigent portfolio of external media includes flash drives, external storage, and SD and MicroSD drives.

- **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, and AI secured storage.

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

  Key features include full drive hardware encryption with PBA, enterprise management, hidden partitions, cloning and wipe prevention, 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.

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 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!