PROTECT DATA AT THE EDGE
PROTECTING YOUR DATA, ENABLING YOUR MISSION

Unmanned vehicles have already established themselves as an essential element in military and civilian operations. Rapid improvements in their capabilities will accelerate adoption for a variety of tasks. Sensitive data on these devices may include valuable proprietary algorithms, mission information, and data gathered during the mission.

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 Secure 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. Partitions 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. Crypto erasure executes in fractions of seconds. 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, crypto and full block erasure.

  The Secure Drive 2230 utilizes the same architecture as Cigent Secure Storage 2280 which is CSfC DAR component list. This includes Cigent PBA with MFA.

- **Secure Drive SSD BGA Encrypted Alpha.** Meets automotive temperature standards (-40 to 105 C). Features include hardware encryption, enterprise management, 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.

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!