

## PROTECT DATA AT THE EDGE

### PROTECTING YOUR DATA, ENABLING YOUR MISSION

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.

**Cigent Secure Storage SSD BGA Encrypted** is designed for use in manned and unmanned vehicles, provides 1 TB of storage and meets automotive temperature standards (-40 to 105 C).

#### Features:

- **Full Drive Hardware Encryption:** 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.
- **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 drive preventing even sophisticated adversaries from compromise.
- **Hidden Partitions:** 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:** Data at rest protection is protected with full drive hardware encryption that locks all ranges. Cigent is unique in also preventing cloning and wiping 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:** provide the ability to locally or remotely execute a cleanse that erases all data via crypto and 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.