CIGENT AlwaysPROTECTED™

PROTECT DATA AT THE EDGE
Protecting your data, enabling your mission

Data at Rest Protection

Introduction

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.
This document briefly explores the importance and challenges of securing data on devices operating at the edge including protecting data at rest (DAR) and throughout its lifecycle. It will overview Cigent Secure Storage Solutions and the features that allow you to confidently deploy data on edge devices.

Threat Environment

Mission requirements and rapidly evolving technology has accelerated the deployment of devices operating in unprotected environments. Sensitive data will be collected, processed, and stored on these devices resulting in risk of unauthorized data access when adversaries gain physical access. The number and types of devices are undergoing a rapid expansion including traditional compute devices - PCs, Servers, External Media and non-traditional - Manned and Unmanned Vehicles, and Industrial Control Systems.

Threat actors utilize a variety of technology and methodologies to compromise data on these devices. Threats include scan disk cloning, low pin count (LPC) bus sniffing, hex editors, and firmware tampering. These technologies are widely utilized and are capable of compromising widely utilized full drive encryption (i.e Microsoft BitLocker) . More advanced threat actors may employ techniques including the use of electron microscopes to access data. And with the rapid progress of quantum computing there is an emerging threat to traditional cryptography.

The combination of more devices operating at the edge (collecting, processing and storing a greater volume of sensitive data) with great adversary motivation to compromise the data and employing more advanced capabilities to overcome traditional protections, creates a challenge for project managers to ensure the integrity of data at rest.

Threat Environment

Operating in this difficult threat environment, project managers will need to consider a number of factors to ensure appropriate data protection:

- What devices will have data that need to be protected? It is no longer only traditional compute devices (i.e. PCs). Any device that stores sensitive data needs to be protected.

- What devices will have data that need to be protected? It is no longer only traditional compute devices (i.e. PCs). Any device that stores sensitive data needs to be protected.
- What are the administration and reporting requirements? Need an efficient management approach to address administration.
- How do I ensure that addressing data security does not adversely impact operators? It is critical that the user experience (UX) is intuitive and straightforward.
- What are the different threats? Protection for DAR is an absolute requirement but consideration is protecting data throughout its lifecycle.
- How will I sanitize data? Upon mission completion or in an emergency situation it is imperative to ensure the data cannot be recovered.

Cigent Solution

Cigent protects data at the edge offering the only integrated hardware and software solution that protects data throughout its lifecycle. The solution utilizes layers of protection to ensure DAR is secured from sophisticated threat actors utilizing advanced data recovery. Cigent Secure Storage also protects data while the device is in use and has patented capabilities to ensure proper data sanitization.

Data-at-Rest Protection

Cigent Secure Storage uses proven and NSA-validated encryption methodology, including full drive AES-256-bit hardware encryption. This encryption is enabled and decrypted by authentication using Cigent’s CSfC-certified pre-boot authentication (PBA) software.

PBA ensures a secure user authentication platform that only allows the trusted user to decrypt the drive. The PBA software has been validated to meet FIPS CAVP, NIAP Common Criteria FDE_AA, and CSfC DAR Capabilities Package 5.0 requirements. On startup, the underlying disk will be fully locked and inaccessible, except for a read-only storage range that contains the PBA platform itself. The rest of the ranges on the drive are locked at the range level of the storage, effectively making the ranges and, therefore, all the software (O/S, applications, configurations, etc.) inaccessible to the device, and thus the adversary.

In the “locked” state, the drive cannot be cloned, wiped, or viewed with any low-level tools such as a hex reader. The data on the drive in these ranges is encrypted, preventing an advanced direct physical attack, such as techniques including ‘chip-off’ and using electron microscopes to view and extract the data. Therefore, no decrypted data is accessible until proper authentication, preventing unauthorized access attempts to the system and the physical storage device. Cigent complements its security with a patented portfolio of data protection features to ensure sensitive data remains secure in all aspects of an operation.

Data Lifecycle Protection

Cigent Secure Storage uses proven and NSA-validated encryption methodology, including full drive AES-256-bit hardware encryption. This encryption is enabled and decrypted by authentication using Cigent’s CSfC-certified pre-boot authentication (PBA) software.

While the focus may be on DAR, Project Managers should ensure that data is protected throughout its lifecycle. Cigent’s integrated solution is unique in providing features that addresses threat when the device is in use, mitigates insider threat, and can reliably and efficiently address sanitization requirements.

- **Hidden Partitions:** Cigent Secure Storage provides the option to create hidden, undetectable partitions 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. Valuable for any device operating at the edge, the capability is particularly pertinent to UxV where AI algorithms and mission data needs to be sequestered and hidden.

- **Cloning and Wiping Prevention:** An adversary can execute a cloning or wiping attack in seconds. Cigent partitions lock all data ranges rendering them immune to wiping and cloning of hidden attacks. Data stored in these partitions remain protected even when the device is in use.

- **Data Sanitization:** Data erasure can be initiated locally or remotely to erase data via crypto and block erasure. Additionally, Verified Data Erasures is a patented solution that performs block-by-block analysis to ensure all data has been permanently erased. This capability provides confidence in emergency data destruction situations, addresses risk from emerging quantum capabilities, and provides potential for drive reuse.

- **Secure Data Logs:** collect and securely store all data access activity. The logs are encrypted, preventing a malicious actor from “covering their track.” These logs enable the detection of malicious activity and can be used for forensics in incident response.

Administration

Cigent Secure Storage uses proven and NSA-validated encryption methodology, including full drive AES-256-bit hardware encryption. This encryption is enabled and decrypted by authentication using Cigent's CSfC-certified pre-boot authentication (PBA) software.

Beyond the encryption of data, organizations are also 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.

Cigent Advantage

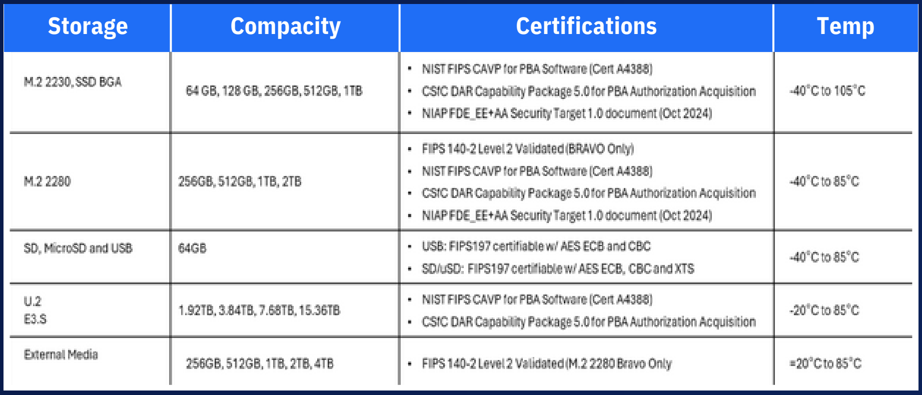
Cigent emerged from the leading experts in data recovery and sanitization with decades of practical experience working with US Federal Agencies. The Cigent portfolio has been thoroughly tested and validated by leading Federal agencies including MITRE, NIST, NSA, NIAP, the Air Force, Cyber Resilience of Weapon Systems (CROWS), and NSSIF (UK).

Cigent drives are available from leading device manufacturers including Dell, HP, and Getac.
If your mission requires unique data protection capabilities, Cigent will work with you on a customized solution to meet your specific requirements. Cigent has the staff, facility, and experience to develop solutions for sensitive mission requirements.

Cigent Portfolio

Cigent emerged from the leading experts in data recovery and sanitization with decades of practical experience working with US Federal Agencies. The Cigent portfolio has 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).

Cigent drives are available from leading device manufacturers including Dell, HP, and Getac.
If your mission requires unique data protection capabilities, Cigent will work with you on a customized solution to meet your specific requirements. Cigent has the staff, facility, and experience to develop solutions for sensitive mission requirements.



Storage	Compacity	Certifications	Temp
M.2 2230, SSD BGA	64 GB, 128 GB, 256GB, 512GB, 1TB	• NIST FIPS CAVP for PBA Software (Cert A4388) • CSfC DAR Capability Package 5.0 for PBA Authorization Acquisition • NIAP FDE_EE+AA Security Target 1.0 document (Oct 2024)	-40°C to 105°C
M.2 2280	256GB, 512GB, 1TB, 2TB	• FIPS 140-2 Level 2 Validated (BRAVO Only) • NIST FIPS CAVP for PBA Software (Cert A4388) • CSfC DAR Capability Package 5.0 for PBA Authorization Acquisition • NIAP FDE_EE+AA Security Target 1.0 document (Oct 2024)	-40°C to 85°C
SD, MicroSD and USB	64GB	• USB: FIPS197 certifiable w/ AES ECB and CBC • SD/uSD: FIPS197 certifiable w/ AES ECB, CBC and XTS	-40°C to 85°C
U.2 E3.S	1.92TB, 3.84TB, 7.68TB, 15.36TB	• NIST FIPS CAVP for PBA Software (Cert A4388) • CSfC DAR Capability Package 5.0 for PBA Authorization Acquisition	-20°C to 85°C
External Media	256GB, 512GB, 1TB, 2TB, 4TB	• FIPS 140-2 Level 2 Validated (M.2 2280 Bravo Only	=20°C to 85°C