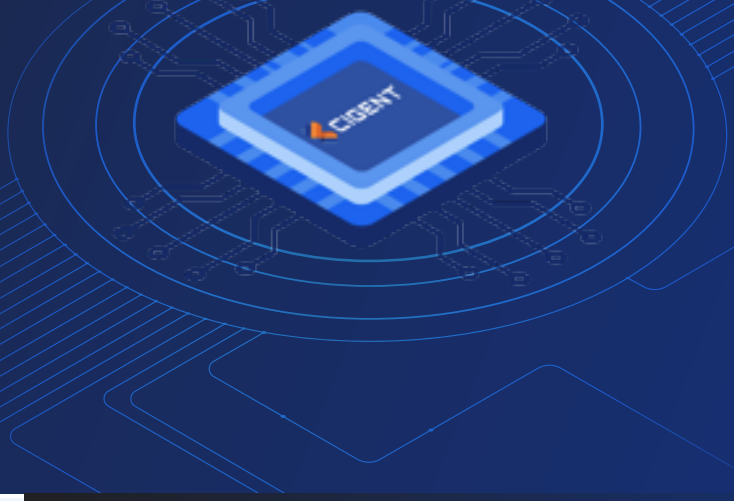
CIGENT

CIGENT DATA DEFENSE™ FOR GOVERNMENT



Solution Brief

PROUDLY FUNDED BY

iqt IN-Q-TEL

The Challenge

Sensitive data in government agency systems and carried by field personnel is always in the crosshairs of our adversaries. These computers and removable media they utilize can hold some of our nation's most valuable secrets. If an adversary gains access to this information, not only will they be privy to the sensitive data, but critical government systems and even human assets may also be compromised. A breach could compromise national security and potentially put lives in danger.

Our Solution

Cigent Data Defense provides advanced security controls to protect, hide, and destroy sensitive data on workstations, PCs, mobile systems and removable data stores. These capabilities enable sensitive systems' data, mission devices, and the personnel that carry them, to avert compromise during departmental operations and in the field.

How it Works

Cigent Technologies uses an integration between the Cigent Data Defense software and SSD media firmware. This integration enables data security to be embedded within the drive itself, providing encryption and strong access controls at the drive, partition, folder, and even the file layer. These capabilities make several use cases available to help protect sensitive data from even the most sophisticated adversaries.

Pre-Boot Authentication (PBA)

Cigent Pre-Boot Authentication (PBA) hardware full drive encryption (HWFDE) leverages the high-performance Self Encrypting Drive (SED) capabilities to encrypt the entire drive. The PBA solution takes this one step further by locking down the all the data ranges of the drive at the hardware layer to ensure the data at rest (DAR) is safeguarded from unauthorized access, cloning, wiping and hex reader utilities. When an authorized user authenticates using Cigent PBA, the drive unlocks and boots normally.

Cigent PBA, combined a compliant SED drive. enforces authentication to the "outer" layer (per CSfC 5.0 Data at Rest Capabilities Package) before the user can access the drive. Upon powering on a system, Cigent PBA prompts the user to authenticate. The PBA solution supports multiple forms of authentication including username and password or CAC/PIV/Yubikey or both (to meet the strictest interpretations of the NIST MFA guidelines).

The PBA solution addresses the high standards for government usage. This includes being certified for Commercial Solutions for Classified (CSfC) DAR, National Information Assurance Partnership (NIAP) Common Criteria, and FIPS validation for cryptographic algorithms, and FIPS 140-2 Level 2 hardware tamper-evident designs (when used in conjunction with a DIGISTOR or Seagate Level 2 certified drive). And, when used in tandem with a FIPS validated drive, Cigent software automatically configures the drive to operate in "FIPS mode" to ensure the highest level of available security is enforced.

Secure Vaults

Secure Vaults provide an additional "inner" layer of security by creating a virtual partition that is invisible to users and the operating system until it is unlocked with step-up authentication using a 2nd authentication factor. Contents of the secure vault data are encrypted and not accessible while locked, even when using drive utilities or alternate operating systems. They also cannot be cloned or "wiped" by malware or drive utilities.

Command Line Interface (CLI) For Secure Vaults

Secure Vaults can also be managed using the Cigent CLI utility. The utility can be used to create up to eight Secure Vaults and adds support for Linux operating systems. The command line utility is ideal for headless environments or for usage in automated processes (such as backing up to a dedicated, hidden partition).

True Erase™

This Cigent solution provides unique capabilities to ensure that data will truly be erased from drives so that they can be reused or disposed of. These include the following:

Cryptographic Erase (CE) – Rapidly sanitizes drives by deleting the key used to decrypt the data. The encrypted data remains present on the drive, the data cannot be decrypted making the recovery of data infeasible.

Full Block Level Erase – A more comprehensive approach to data erasure, this initiates a hardware low-level format of the media. The process performs a secure erase that destroys all data and metadata on the drive.

Complete Erasure Verification – This patented Cigent technology verifies that every block on the drive has been "wiped" after a full block erasure. The verification enables the drive to be safely repurposed or retired with assurance that all data has been completely removed.

Zero Trust File and Folder Access

In addition to FDE and Secure Vaults, Cigent enables an additional layer of security controls at the file and folder level. Folder and individual files can be designated for Zero Trust protections, requiring the user to use step-up authentication to access them. Cigent Data Defense also automatically applies these protections by file type and/or location. For example, Data Defense can be configured to protect all files with a .XLS extension or within the Documents folder.

Shields Up™ Mode

Data Defense is configured by policy in the management console to put protected files and folders into a risk-based, threat-aware state. During normal operations ("peace time"), users work as they always do with no impact to their user experience. During a Shields Up condition, users will be required to use step-up authentication to access protected files. Data protection policy can be set by file type (extension), folder, and partition (Cigent Secure Vault). The protection can also extend beyond files on the local PC to cover file shares, cloud-synchronized files (e.g., OneDrive), and external media.

Additional Capabilities

Service Monitoring – Cigent Data Defense maintains an active "heartbeat" between the Cigent Data Defense service and the drive firmware. In the event the service is disabled (by an attacker or insider), the Cigent Secure Vaults lock at the storage layer, instantly making its content inaccessible to threat actors.

File Encryption – Individual files can be protected with FIPS 140-2 Level 1 validated AES 256-bit encryption that is completely transparent to the user.

Immutable Data Access Logs – Enables administrators to view data access logs maintained on the drive itself, preventing bad actors and insiders from "covering their tracks."

Authentication Options – Unlocking protected files and folders requires the user to step-up authenticate. Data Defense supports multiple options and can leverage the authentication factors you already have. Options include the following:

- PIN - Using the Data Defense client
- Authenticator Apps – Google Authenticator, Microsoft Authenticator, Duo Security by Cisco, and others
- Windows Hello – Authenticate with preferred Windows sign-in option
- Personal Identity Verification (PIV) devices such as a YubiKey
- Common Access Cards (CAC) smartcards

Inquiries

Phone: 669-400-8127
Toll Free: 1-844-256-1825
www.cigent.com

Email:
General Inquiries - info@cigent.com
Sales Inquiries - sales@cigent.com
Partner Inquiries - partners@cigent.com

Locations

Headquarters
2211 Widman Way, Suite 150
Fort Myers, Florida 33901

R&D
402 Amherst St, Suite 402
Nashua, New Hampshire 03063