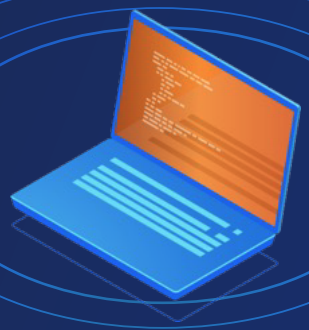
CIGENT
Data Security that Works.™

CIGENT DATA DEFENSE™ PRE-BOOT AUTHENTICATION

For Hardware-Based Full-Drive Encryption

Solution Brief

PROUDLY FUNDED BY
iqt IN-Q-TEL



The Challenge

Data is the most valuable asset and stealing it has become a top objective for cybercriminals. Data-at-rest (DAR) encryption helps to safeguard data when a device is stolen, however software-based DAR solutions, that utilize OS credentials, are more vulnerable to cyber criminals. Account credentials are regularly compromised (e.g., phishing) and advanced attackers can even circumvent the Windows login prompt, leaving the DAR controls ineffective and the system wide open to attackers.

Our Solution

Cigent Pre-Boot Authentication (PBA) for Hardware-based Full Drive encryption (HWFDE) provides an additional security layer of pre-boot authentication for systems with encrypted drives. Transparent to the OS, Cigent PBA stops cyber criminals from accessing protected systems and devices, even if the Windows credentials have been compromised. Using proven security, the solution meets the rigorous US government standards for user authentication and protection of Classified and Top-Secret data.

How it works

Cigent Data Defense Pre-Boot Authentication (PBA) enables data at rest (DAR) to be fully protected from adversaries if they get physical access to the system or the storage device. PBA leverages self encrypting drive (SED) capabilities to encrypt the entire drive. The PBA solution takes this one step further by locking down the the data ranges of the drive at the hardware layer to ensure the data at rest (DAR) is safeguarded not only from unauthorized access, but also cloning, wiping and hex reader utilities.

When an authorized user authenticates using Cigent PBA, the drive unlocks and boots normally. PBA is independent of the device's OS. The Cigent PBA controls cannot be disabled from within the OS itself, ensuring that the security cannot be disabled by users or malware. The solution supports both Windows and Linux.

Protect Data with Trusted Security

The security built into the Cigent solution is trusted to secure sensitive data for enterprises and government agencies. Built for both high performance and security, the protection combines the drive's native hardware-based 256-bit AES encryption with Cigent's provide strong and trusted encryption for protecting highly sensitive data.

Meet Rigorous Security Standards

The solution addresses the high standards for government usage. This includes meeting the requirements for Commercial Solutions for Classified (CSfC) DAR, National Information Assurance Partnership (NIAP)[1] Common Criteria, and FIPS validation for cryptographic algorithms[2]. And, when used in tandem with a FIPS validated drive, Cigent software automatically configures the drive to operate in "FIPS mode," simplifying the process to operate the system with higher assurance or in environments where FIPS operation is mandatory.

[1] CSfC DAR Capabilities Package 5.0 compliant Full Disk Encryption protection with FDE_EE and FDE_AA NIAP Protection Profiles compliance.
[2] Cryptographic Algorithm Validation Program https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?validation=35911

Administrative Management

Cigent includes an administrative console to manage users and features. From within the console, administrators can set authentication policies such as password rules, password reuse, authentication methods, and number of failed logins before drive erasure. Administrators can also add, remove, or modify user accounts on individual systems as well as uninstall, disable, or crypto erase a drive.

Administrative tools also include access to activity log data to see the devices authentication activities, such as failed login attempts.

True Erase™

Integrated into the management console, the Cigent solution provides unique capabilities to ensure that data can be truly erased from drives so that they can be reused or disposed of. These include the following:

Cryptographic Erase (CE) – CE is a method of rapidly sanitizing drives by deleting the key used to decrypt the data. The encrypted data remains present on the drive, however without the decryption key, the data cannot be decrypted making the recovery of data infeasible.

Full Block Level Erase – This function takes a more comprehensive approach to data erasure. The Cigent solution initiates a hardware-based 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 function. The verification enables the drive to be safely repurposed or retired with the assurance that all data has been completely removed and is unrecoverable. Complete Erasure Verification works on any Cigent Secure SSD.

Advanced Features with Secure SSDs

Cigent's Data Defense cybersecurity capabilities are embedded in the firmware of popular, market-leading SSDs. When Cigent Data Defense software is used with one of these drives, the combination enables additional protections and features including:

Cigent Secure Vaults – Part of the Cigent Data Defense software, 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 the Cigent Data Defense software and MFA. 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 by drive cloning software or wiped by drive wiping software (without Cigent Data Defense).

Immutable Insider Threat Data Access Logs – This feature enables administrators to view data access logs maintained on the drive itself, preventing the ability for bad actors to "cover their tracks." These logs provide details of the drive activity, such as recent file access, even if the system has been booted from an alternative OS (e.g., USB) drive.

Automated Threat Response in Storage – Secure SSDs[3] incorporate a heartbeat between the drive firmware and the Data Defense software service. In the event the Data Defense service is disabled (by an attack or insider), the drive firmware automatically locks Cigent Secure Vaults at the storage layer, instantly making Secure Vaults and their content inaccessible to threat actors. This advanced hardware and software intregration adds higher levels of security than software only architectures.

[3] Complaint with the Trusted Computing Group (TCG) Opal Security Subsystem Class (SSC) specification

CIGENT®
Data Security that Works.™

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