



# Superior Data Defense For Sensitive Federal Devices

## ENDPOINT DATA RISK





In the field, the endpoint devices used by your teams represent a significant vulnerability. [73% of endpoint devices](#) contain sensitive data which can compromise your mission if it gets into the wrong hands.

[70% of successful data breaches](#) occur at endpoint devices and those devices are high-theft items, with [17% of data breaches](#) occurring due to lost or stolen devices. Even the most highly-trained individuals can have their devices targeted, so protecting the data contained on them is critical.

## DATA DEFENSE

It's a fair assumption that you're going to deal with missing endpoint devices at some point, so the question is how to keep the data safe, even if a malicious actor has the actual device. Fortunately, Cigent's NSA-sanctioned Data Defense makes that possible.

### Our "4 protects" are our cornerstones:

-  Protects - Even when the device is compromised.
-  Protects - Against all forms of attacks.
-  Protects - Data with minimal impact on user experience.
-  Protects - Without administrative oversight.

Cigent uses layered protections to keep data safe. Controlled access means that even if an unauthorized person unlocks the device, they can't access the data. Secured, hidden drives mean that malicious actors can't compromise what they can't see.

## HOW DATA DEFENSE WORKS

Cigent Data Defense is deployed as a Windows agent without end user configuration or interaction. Once deployed, Cigent can protect against unauthorized access of sensitive data, such as through ransomware or data exfiltration.

The protections Cigent can provide can be persona-based via policy settings. They can be set in a couple of ways:

- Silently in the background until a threat event is occurring.
- With policy settings in place to be more proactive. These require authentication depending upon the data being protected.
- These protections can be extended from both a pre and post boot state.

## DETAILED CAPABILITIES

### Step-Up Authentication

- Protect federal data from unauthorized access. Integrates with Windows Hello, Authenticator Apps (e.g., Google, Microsoft), Duo, Common Access Card (CAC) and Personal Identification Verification (PIV) devices (e.g., YubiKey).

### Instant Protections

- Provides protections for a predefined set of file types (92 different file types).
- When a threat has been detected protections automatically shield those file types, and require step-up authentication to access. Additional files can be added to the protections
- Protections can be applied to a single endpoint or to all Cigent managed machines.

### File Type and Folder Protections

- Protect data within folders using step-up authentication.
- Define when a user should be prompted for authentication: Every time, during a threat, or after so many files have been opened within a timeframe.
- Protect files by type (e.g., PDF, Word, Excel, proprietary or custom). File type rules are not bound by location (like folder rules).

### File and Folder Encryption

- FIPS 140-2 Level 1 validated AES-256 encryption to encrypt files within folders, as well as individual files (for external sharing).

### Sensors

- Data Defense uses deception technologies at the file and network levels. If an attacker is doing reconnaissance on the network or within the file and folders on an endpoint, Data Defense can detect and start to prevent further damage from happening on the endpoint, while alerting others.

- Additionally, Cigent Sensors can integrate with security solutions (e.g. Microsoft Defender, SentinelOne) which registers with the Windows Security Center. When those solutions detect a threat and/or their underlying service is stopped, Cigent will detect the threat and immediately put the endpoint into a Shields Up mode.

### **EDR Integration**

- Data Defense can integrate with leading EDR solutions via RestAPI's to provide a last line of defense for data protection if the EDR solution detects a threat.
- When the EDR solution detects a threat, Cigent will then go into a Shields Up mode and protect corporate endpoints. It can provide protections for the endpoint that detected the threat, endpoints in the assigned group of the initial device or all corporate endpoints.

### **Secure Vaults**

- Data within TCG Opal 2.0 SED's can be partitioned to create secure vaults. The secure vaults are invisible to both the Operating System and threat actors. While locked in the secure vaults the data is encrypted using AES-256 encryption.
- The Secure Vaults can only be opened using the end-users Step-Up Authentication factor. During a threat the Secure Vault(s) will automatically lock.
- If attempts are made to clone or wipe the drive, the partitioned data cannot be removed.

### **Command Line Interface (CLI) Tool**

- The Cigent Command Line Interface (CLI) is a standalone utility, which can manage Cigent Secure Vaults in supported Self-Encrypting drives. Those include Cigent or Cigent partners, such as Digistor or Seagate.
- The CLI utility can be used to configure and create up to eight Secure Vaults (varying in size) and adds support for Linux operating Systems (Ubuntu and RHEL). Additionally, the CLI utility can be used to de-configure Secure Vaults through different CLI functions, including PSID Revert, and Erase. This includes a cryptographic and full-block erasure.
- The CLI Utility supports the Cigent Pre-Boot Authentication (PBA) solution and can be used in conjunction with PBA to provide pre and post boot protections.

## **GET STARTED WITH CIGENT**

Cigent stands ready to protect all of your endpoint devices from all forms of malicious attack. [Schedule a demo](#) with us today to get started.