

Cigent D³E

Take Windows 10 data defense to a new level.

Extend zero trust to the data layer.

The Cigent Dynamic Data Defense Engine™ (D³E) is a new approach to data security, one that relies on cybersecurity best practices, including zero trust, continuous authentication, deception, and threat intelligence—and applies them as close to the data stream as possible. Cigent D³E ensures your data remains secure, even when your system is under duress or your credentials have been compromised. And Cigent D³E plays well with others, complementing security solutions you already have in place. The result is an unprecedented level of protection, detection, and response to cyberattacks, insider threats, and lost or stolen devices.

Gain critical endpoint and external media data security with Cigent D³E.

Secure Data with Minimal Impact

Protect files on endpoints and external media with D³E. Featuring a simple, yet highly effective approach, D³E doesn't block file use or quarantine systems and requires little-to-no IT or SOC involvement.

Ransomware Prevention

The simplest and most effective approach to prevent ransomware from encrypting your files is to block it from accessing them in the first place.

Insider Threat Prevention

D³E detects and prevents data exfiltration attempts in real time by malicious insiders by ensuring that only the trusted user can access their files.

Threat Intelligence

Respond quickly and effectively to threat intelligence with file locking, either locally or across groups of users. Detailed global threat activity is captured and stored permanently in the cloud—searchable using filters, dashboards, and alerts. Import and export data to other security consoles and tools via REST APIs.

Compliance

Address critical requirements for data governance and privacy programs—such as CMMC, HIPAA, GDPR, GLBA, PCI-DSS, and CCPA—by securing endpoint data effectively.

Easy Policy Setting

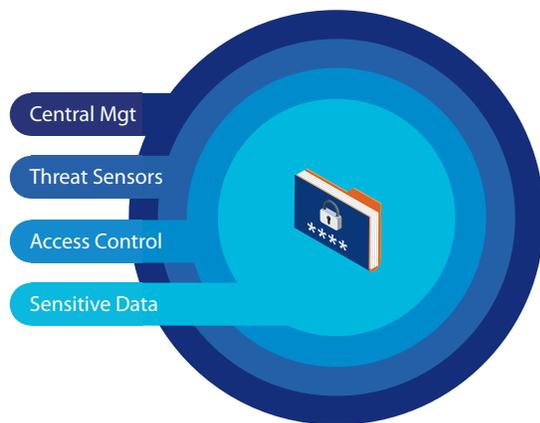
Set policies and roll your baseline D³E configuration to specific groups or organization wide, including to groups who are working from home. For teams that save sensitive files regularly, set D³E to automatically protect files stored in designated folders or by file type. Non-intrusive and end-user friendly, D³E automatically raises protections when threats are detected.

Protect your data from the inside out.

Cigent D³E is always on the job.

See how Cigent D³E works.

D³E relies on zero-trust file-access controls in order to protect sensitive files on Windows 10 devices. When the user tries to access a file that's protected by D³E, a step-up authentication is required to prove the person's identity. This simple but powerful approach to data defense is immediately effective, preventing data theft perpetrated by a myriad of cyberattacks, including advanced malware, ransomware, malicious insiders, unpatched software vulnerabilities, stolen credentials, and more.



Cigent Active Lock

The Active Lock response feature is a powerful—yet user friendly—approach to preventing unauthorized access to your most treasured data.

Trusted users are always allowed to access individual files with a step-up authentication. There are two types of file protection modes available:

Always Locked Files

- Files remain locked under all conditions
- Step-up authentication is required to access individual files
- Designed for extremely sensitive information

Dynamically Locked Files

- Files are locked only if a potential threat has been detected.
- Designed for sensitive files that are accessed frequently
- Provides strong protection in a minimally invasive manner—the user is prompted to authenticate only if a threat is detected

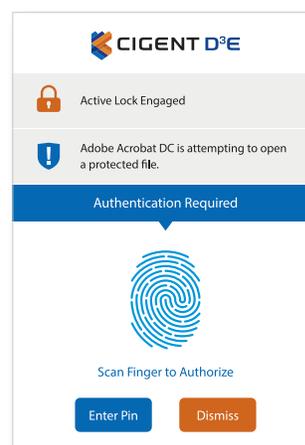
Authentication Options

A minimally invasive step-up authentication is required to access locked files. Authentication methods include, but are not limited to:

Windows Hello (Facial Recognition, Fingerprint, PIN)

Google Authenticator

Third-party authentication methods, such as Cisco Duo



Count on rapid, granular response.



Protect your data from end to end.

Cigent Dynamic Mode Threat-Sensor Platform

Cigent D³E relies on a variety of native and third-party sensors to detect signs of compromise. When the threat level is elevated, dynamically protected files are automatically locked until the threat is cleared.

- Ransomware, malware, fileless attacks, privilege escalation¹
- Endpoint security agent disabled
- Untrusted network detection
- External media insertion detection
- Network and file deception engines
- AI-based machine learning sensors (keyboard typing, network usage)
- Ransomware detection based on file access patterns

¹Third-Party Integrations

Sophos	VMWare Carbon Black
Windows 10 Security	PC Matic
CyberArk	And more

Granular File Protection

Sensitive files can be designated for protection by file type or folder type.

File Type:	Microsoft, Adobe, Custom
Folder Type:	Always Locked, Dynamically Locked

Optional Cigent DataSafe K2 Storage

For added security, Cigent offers a family of internal and external SSDs—the industry's first storage appliances with built-in cybersecurity. When paired with D³E, Cigent DataSafe™ includes the following firmware-based features:

Secure Drive

Adversaries can't steal files that they can't see. When used in conjunction with D³E, Cigent DataSafe storage supports the creation of Secure Drives—self-encrypting disk partitions that can be used to securely store your sensitive files below the OS layer. Secure Drives are threat aware and disappear whenever a threat is detected or the PC is power cycled. The effect of these security measures is that sensitive files are accessible for a very limited time and only on an as needed basis.

Keep Alive

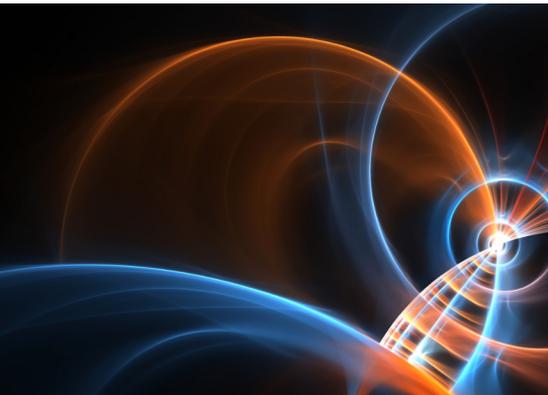
Common techniques of attackers include disabling security software, booting from an alternate O/S, and removing the drive. Cigent DataSafe uses a Keep Alive heartbeat in the firmware that constantly ensures designated cybersecurity software is running, including D³E. If not, all Secure Drives automatically lock and can not be bypassed.

Data Access Log Protection

Advanced attackers almost always wipe their tracks, deleting system and data access logs. Cigent DataSafe Storage captures and protects comprehensive, firmware-secured data access logs and audit trails that cannot be wiped. Access logs are stored for incident response, non-repudiation, and litigation use.

Firmware-Verified Storage Erasure

Cigent DataSafe storage is the first and only SSD to include Cigent TrueErase™ firmware verification that reports each block's erased or unerased state after a wipe attempt. TrueErase, allows the trusted user to safely repurpose their device, retire it, or ship it for destruction, saving money on expensive media and allowing you to implement a green policy to storage device lifecycle management.



Cigent D³E

About Cigent

Cigent Technology keeps the most valuable asset on your endpoint safe—your data. Our cybersecurity solutions are built by an elite team, with backgrounds in intelligence, ethical hacking to help public and private entities protect themselves, and data storage, including development, erasure, and recovery. As a result, our solutions beat hackers at their own game, and keep your data safe.

Contact us

Cigent Technology Inc.
2211 Widman Way Suite 150
Fort Myers, Florida 33901

Phone: 669-400-8127
Toll Free: 844-256-1825

Email us

General Inquiries
info@cigent.com

Sales Inquiries
sales@cigent.com

Partner Inquiries
partners@cigent.com

Visit us online

www.cigent.com

Cigent D³E Personal

The Cigent D³E End-User Dashboard makes it easy to designate protected files by file type, folder type, and always locked vs dynamic modes. The D³E End-User Dashboard also allows the user to create data deception files, set up Secure Drives, and configure authentication methods. Popular Windows 10 file types, including Microsoft Office and Adobe, are dynamically protected out of the box. Cloud storage solutions can sync to local folders without authentication and files that are stored in local Dropbox, OneDrive, and Google Drive folders can be protected.

Cigent D³E Business

The Cigent D³E Enterprise-Ready Management Console supports flexible deployment, configuration, and response. As a result, user requirements are easy to accommodate, and sensitive corporate data is easier to protect.

Device Management

View Active Lock, policy compliance, and protection status across all devices. Easily identify devices that are not meeting minimum protection standards and those that should have incremental protection configured.

Centralized File Locking

To ensure rapid response to externally-detected threats, engage Active Lock on a single device or on a group of devices—quickly and easily.

Threat History

View historic threats across all devices. Use predefined filters or Google-style search to quickly refine your search.

Notification

Upon login, users are notified of any new threats that have been reported since they last logged in. To stay abreast of newly detected threats at all times, subscribe to hourly email notifications.

Device Sets

To facilitate better policy and threat-response management, organize devices into logical groupings.

Enforce Policies

Assign minimum protection settings either globally or by device set. Take advantage of predefined, customizable protection for Microsoft Office and Adobe files. Load a protection configuration from an existing device and use it as a policy template.

Integrations

Configure and manage integrations to other endpoint detection and response solutions—such as VMware, Carbon Black, Sophos, PC Matic, and CyberArk—to enable an additional layer of response to threats detected by those solutions.

