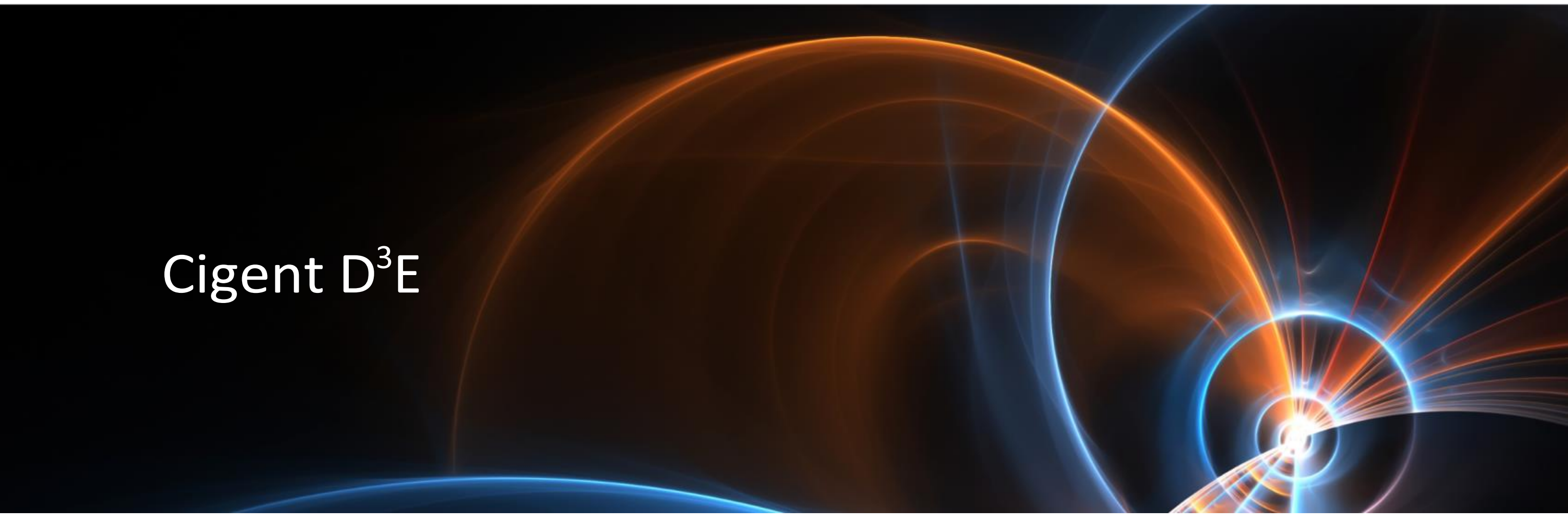


Cigent D^{3}E

Take Windows 10 data defense to a new level.

Extend zero trust to the data layer.

The Cigent Dynamic Data Defense Engine™ (D^{3}E) 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 D^{3}E ensures your data remains secure, even when your system is under duress or your credentials have been compromised. And Cigent D^{3}E 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 D^{3}E.

Secure Data with Minimal Impact

Protect files on endpoints and external media with D^{3}E. Featuring a simple, yet highly effective approach, D^{3}E 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

D^{3}E 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

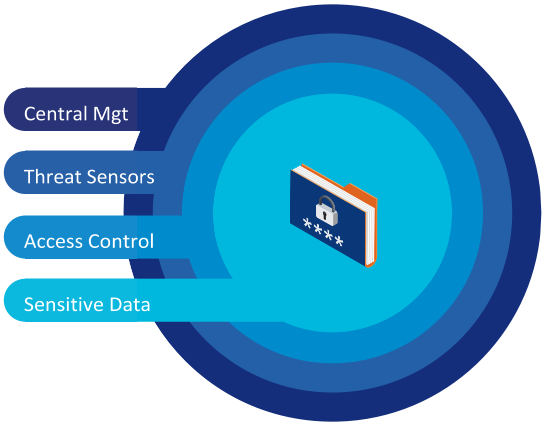
Set policies and roll your baseline D^{3}E configuration to specific groups or organization wide, including to groups who are working from home. For teams that save sensitive files regularly, set D^{3}E to automatically protect files stored in designated folders or by file type. Non-intrusive and end-user friendly, D^{3}E automatically raises protections when threats are detected.

Protect your data from the **inside out.**

Cigent D^{3}E is always on the job.

See how Cigent D^{3}E works.

D^{3}E 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 D^{3}E, 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

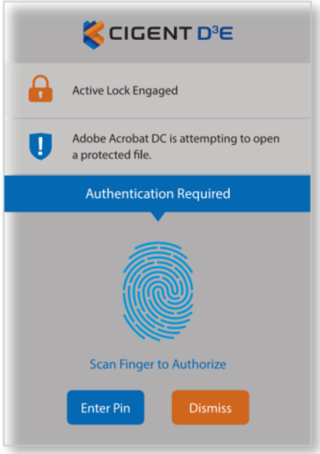
- Files remain locked under all conditions
- Step-up authentication is required to access individual files
- Designed for extremely sensitive information

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:



CIGENT D^{3}E

Active Lock Engaged

Adobe Acrobat DC is attempting to open a protected file.

Authentication Required

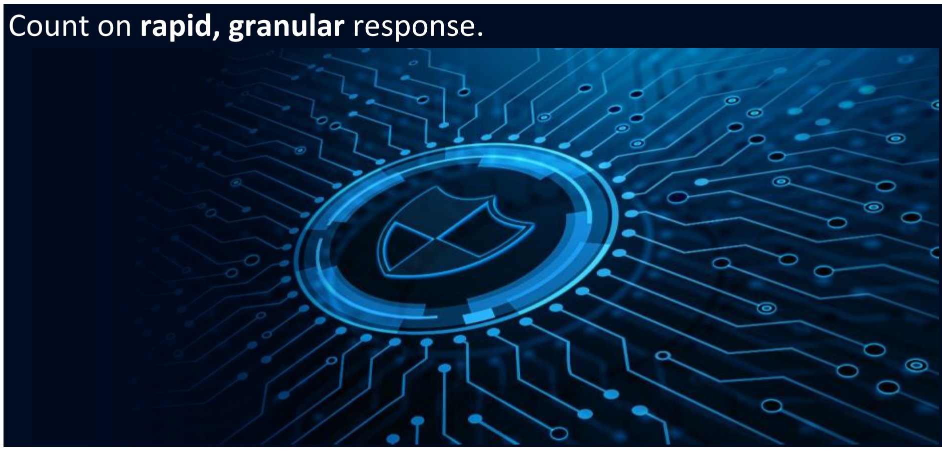
Scan Finger to Authorize

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 D^{3}E 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 escalation[1]
- 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

[1]Third-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 D^{3}E, 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 D^{3}E, 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 D^{3}E. 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.