CIGENT

CIGENT SELECT
Data Sheet

PROUDLY FUNDED BY

iqt IN-Q-TEL™

File Security on Your PC and Wherever Files Go

Protect any file on your PC, clouds, and wherever files go with file encryption, zero trust file access, and secure file sharing. Optionally, use an Opal SED to make files invisible protected by tamper-proof credentials.

Protect Data Wherever it Goes

DLP is complex to manage and too restrictive for users.

Stop Ransomware and Remote Attacks

EDR is not working. Cyber attackers can easily compromise your endpoint.

Stop Physical Data Exfiltration

FDE and SEDs can be easily defeated, thus exposing your data when your device is lost, stolen, or confiscated.

Impossibly Secure™

Render your data invisible. Attackers cannot compromise what they cannot see.

Cigent® protects your most valuable asset—your data. Using advanced, military-grade data security, Cigent protects data against any threat vector. Backed by In-Q-Tel, Cigent solutions are created by an elite team of experts in storage, data forensics, and cyber security. When you need security solutions that protect your most valuable asset, trust Cigent to keep your data safe.

CIGENT CAPABILITIES

Cigent provides a single solution with layered protections defending against all data attacks.

Cigent Select protects files from data theft on PCs, clouds, and wherever files go with file encryption and digital rights management, ensuring only trusted users can access files. Critical files are always protected against ransomware, and all encrypted files are protected when attacks are detected. Optionally, use an Opal SED to protect against advanced remote and physical access attacks, by storing files in an invisible partition that is only accessible by the trusted user with MFA.

On any Windows PC or Virtual Machine

File Encryption

Files are protected on PCs, when synced to clouds, or if users inadvertently share them with unintended parties

- Users can securely share encrypted files with others or easily decrypt them before sending
- Files include an organization key so colleagues can seamlessly work on files together

Secure File Sharing

Files remain encrypted, only accessible by trusted users, wherever they go

- Protect all file types: Office, Adobe, CAD, images, applications – any file
- Users easily share files outside the organization by adding individuals or groups to the file's trusted user list

Zero Trust File Access

File access controls prevent zero-day ransomware and data exfiltration with file-level MFA

- Critical files always require MFA and all other encrypted files only when threats are detected
- Access files online and offline with PIN, fingerprint, facial recognition, CAC/PIV, and authenticator apps

Keep-alive Heartbeat

File filter driver that prevents file access if Cigent software is disabled

- Protects files against advanced remote data theft and ransomware attacks
- Automatically makes encrypted files inaccessible if Cigent is not running properly

PC with Opal Drive

Invisible Data

Data is invisible, even after logging on until unlocked with MFA

- Storage firmware renders data unreadable at the sector level, preventing all physical and remote attacks.
- Drive can be configured with pre-boot authentication (PBA), rendering the O/S partition invisible.

Tamper-proof Credentials

A novel approach to the creation and storage of credentials that make credential access impossible

- Cryptographically derived from a user-supplied password
- Never stored in their final form
- Use the maximum length allowed by the drive

Opal SEDs are available on all Lenovo ThinkPad PCs and as a configuration option on most Dell and HP PCs as well as from leading storage providers: Samsung, Seagate, Western Digital, Micron, Toshiba, Intel, SK Hynix, Smart Modular, Sandisk, Kingston, Kanguru, LiteOn, Kioxia, Crucial, Union Memory, HGST.

CIGENT PLUS

Multi-tenant, hosted or on-prem SaaS platform with group policy settings, threat and event reporting, and notifications.

For enterprise management of multiple users and enhanced security, choose Cigent Plus

Enterprise Security Capabilities

- Enterprise auth factors: Duo Security by Cisco

- Integration with NGAV and EDR: Cisco Security, Sophos, VMware Carbon Black, Dell Trusted Device, CyberARK, PC Matic

- Whitelist apps for cloud syncing, backups, eDiscovery, etc.

- Automated zero trust and risk-based file access and encryption by folder or file type (Office, Adobe, or custom)

- Enterprise Digital Rights Management: add and deactivate users, enterprise master key to access corporate users' data, file encryption key recovery

- Remotely elevate risk state of endpoints via console (i.e. when SOC determines an eminent threat on user, endpoint, or group)

- RESTful APIs for SIEM integration

- Advanced risk-based threat detection: network/port deception, file deception, new network connections, new removable media insertions

Try Cigent Plus Free for 30 Days

www.cigent.com/product

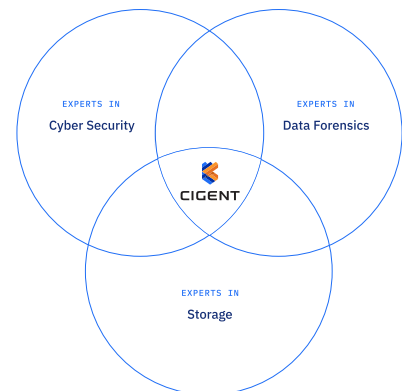### What makes Cigent so effective?

- ✓ We embrace zero trust at the file level
- ✓ We make data invisible
- ✓ We protect the data itself vs. the device or network

Customer Benefits

- ✓ Protects Data from Physical and Remote Attack Vectors
- ✓ Complements Existing EDR and FDE Solutions
- ✓ Protection with Low to No Operational Overhead
- ✓ Available with FIPS 140-2 Certificate

About Cigent

Cigent Technology Inc is a fusion of leading experts in storage, data forensics, and cyber security with an In-Q-Tel-backed mission to commercialize its military-grade technology to provide the most secure data protection available by protecting the data itself from any threat vector.

EXPERTS IN
Cyber Security

EXPERTS IN
Data Forensics

EXPERTS IN
Storage

CIGENT