CIGENT

CIGENT PLUS

DATA SHEET v1.1

PROUDLY FUNDED BY

iqt IN-Q-TEL

Enterprise Data Security and Cigent® Secure SSD™ Management

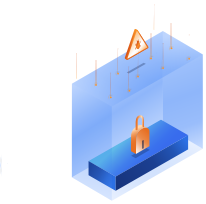
Enterprise-wide data protection from ransomware and data theft on endpoints and wherever files go with file encryption, MFA for file access, and digital rights management. Prevent remote and physical attacks with Opal SEDs and enable advanced protections, including insider threat detection and verified data destruction, on a Cigent Secure SSD.

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.

On any Windows PC or Virtual Machine

Zero Trust File Access

File access controls that only allow the trusted user to access individual files with MFA.

- Consistently defeats zero-day ransomware and data theft for in-use data.
- Files can be configured as risk-based, only requiring MFA when threats are detected.

Secure File Sharing

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

- Protect all file types: Office, Adobe, CAD, images, applications – anything.
- Users easily share documents by adding individuals or groups to the trusted user list.

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.

Hacker-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.

PC with Cigent Secure SSD

Keep-alive Heartbeat

Storage firmware heartbeat that ensures Cigent software is always running.

- Protects against adversaries who disable endpoint security software.
- Makes in-use data invisible if attackers disable Cigent software.

Dual Mode

Two drives on a single SSD with unique O/S' entirely invisible to each other at the BIOS level.

- Enable corporate and personal use without risk of compromise.
- Travel internationally without concern of data loss.
- Create a secret, secure drive that adversaries have no way to know is there.

Verified Data Destruction

Block-level verification that data is irrevocably deleted and unretrievable by any known method.

- Allow for drives to be safely repurposed or retired.
- Saves budget and provides for a greener option.
- Provides emergency data destruction confidence.

Secure Access Logs

Data access logs are securely stored in storage that cannot be wiped.

- Only solution that tracks data theft when insiders boot off a USB stick.
- Prevents insiders or external attackers from "covering their tracks."
- May be used for incident response, non-repudiation, and litigation.

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.

ENTERPRISE MANAGEMENT

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

Enterprise Security Capabilities

- Enterprise auth factors: Duo Security by Cisco, CAC/PIV, PIN, fingerprint, facial recognition, authenticator apps
- 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

What makes Cigent so effective?

- ✓ Our protection begins in storage firmware
- ✓ We embrace zero trust at the file level
- ✓ We protect the data itself vs. the device or network
- ✓ We make data invisible
- ✓ Our credentials cannot be accessed

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.