CIGENT

IMPOSSIBLY SECURE™

Data secured by Cigent® cannot be hacked, ransomed, stolen or exfiltrated as it remains invisible to unauthorized parties protected by tamper-proof credentials and the industry's only zero-trust file level security.

Keeping Data Secure Seems Impossible

Cyberattacks and data breaches are inevitable. Hackers employ various tactics to compromise endpoint devices to access your data. Current protections will continue to be defeated, leaving data vulnerable to compromise. Just one vulnerability opens the door for a physical or remote attack to occur.

Endpoint devices are vulnerable to physical attacks when lost, stolen, confiscated, or compromised by remote access.

Existing protections, including full disk encryption (FDE), self-encrypting drives (SEDs), and endpoint detection and response (EDR), have failed to protect data.

Files are stored in multiple locations and shared with others making them easily accessible to adversaries. Data Loss Prevention (DLP) solutions are complex to manage and too restrictive for users.

? How can you protect your data from the seemingly inevitable data breach?

Secure Your Data with Cigent

Secure your data for confidentiality, integrity, and availability.

Customer Benefits

- ✓ Protects against physical and remote attacks.
- ✓ Delivers protection with low to no operational overhead.
- ✓ Complements existing endpoint detection and response and coexists with FDE.
- ✓ Supports compliance requirements including FIPS 140-2, NIST 800-171, CMMC, GDPR, HIPAA, CCPA, and EO14028.

Single Solution with Layered Protections

- ✓ Invisible Data
- ✓ Zero Trust File Access
- ✓ Secure File Sharing
- ✓ Tamper-proof Credentials
- ✓ Dual Mode
- ✓ Verified Data Destruction
- ✓ Keep-alive Heartbeat
- ✓ Secure Access Logs

ABOUT CIGENT

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

Cigent Solutions

EXPERTS IN
Cyber Security

EXPERTS IN
Data Forensics
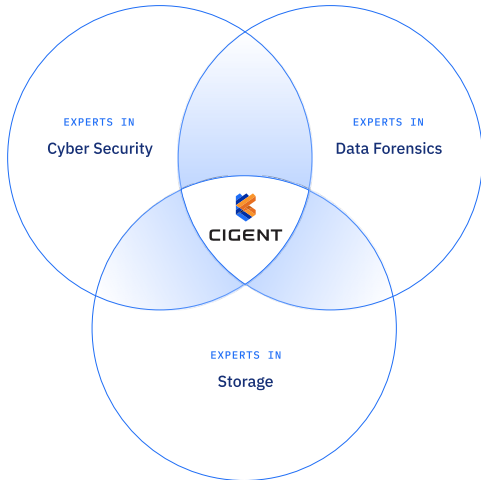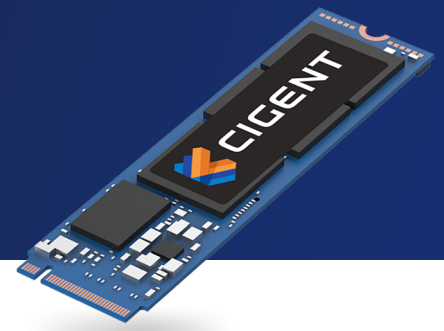
CIGENT

EXPERTS IN
Storage

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 addresses endpoint vulnerabilities by moving from detection and response to protecting the data itself. Cigent's storage security firmware hides critical data from cyber adversaries even when they have physical or remote access to the device.

Wherever files secured by Cigent go, they cannot be accessed by unauthorized users as the data remains encrypted, protected by digital rights management and the industry's only zero trust file access security.

Cigent Capabilities

Prevent data compromise when a device has been lost, stolen, or remotely accessed.
Cigent's layered security capabilities include:

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

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

Secure File Sharing
Files remain encrypted, only accessible by trusted users, wherever they go.

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

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

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

Keep-alive Heartbeat
Storage firmware heartbeat that ensures Cigent software is always running.

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

Your data's confidentiality is secure. Its integrity is secure. Its availability is secure.
Sound impossible? It's not with Cigent.

Inquiries

Phone: 669-400-8127
Toll Free: 1-844-256-1825
www.cigent.com

Email:
info@cigent.com
sales@cigent.com
partners@cigent.com

Locations

Headquarters
2211 Widman Way, Suite 150
Fort Myers, Florida 33901

R&D
402 Amherst St, Suite 402
Nashua, New Hampshire 03063