CIGENT

CIGENT SECURE SSD ADVANCED

DATA SHEET v1.1

FIPS VALIDATED 140-2

PROUDLY FUNDED BY

iqt IN-Q-TEL

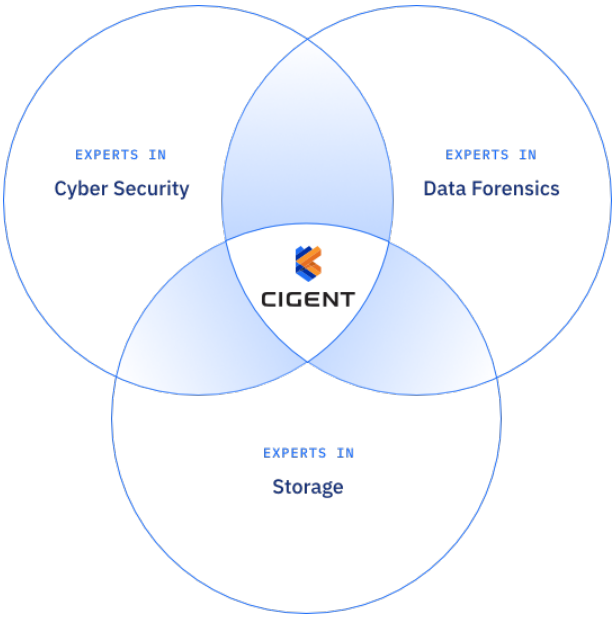
Impossibly Secure™

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.

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.



MARKET SITUATION

Keeping data secure seems impossible. Endpoint devices may be lost, stolen, or confiscated. And files are saved to clouds, networks, removable media, and email making them even more vulnerable to cyber attacks.

Stop Physical Data Exfiltration

Endpoint devices may be lost, stolen, or confiscated. Once adversaries have physical access to a device, neither software full disk encryption (FDE) nor self-encrypting drives (SEDs) will prevent data compromise.

- Variety of methods, including tools like Passware Kits, can be used to circumvent software FDE solutions, including Bitlocker
- Lack of proper IT hygiene creates misconfigurations, configuration drift, security app conflicts, weak credentials, and unprotected BIOS, enabling easy access to data
- More sophisticated methods can defeat SEDs, including weak credential exploitation, brute force attacks, chip off, reverse engineering firmware, and many more
- Work from home increases the risk of adversaries gaining physical access to the device

Stop Ransomware and Remote Attacks

Detect and respond has proven ineffective. Advanced malware, fileless malware, living-off-the-land, zero-day, supply chain, and social engineering attacks can bypass EDR resulting in compromises.

- Attackers able to disable security software
- Vast number of unpatched known and unknown software vulnerabilities
- Sophisticated attackers utilize increasingly specialized tactics and capabilities
- Supply chain and firmware attacks

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

Customer Benefits

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

CIGENT CAPABILITIES

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

Cigent Secure SSD™ Advanced

FIPS 140-2 Validated secure storage with custom firmware and a perpetual software license that protects data from zero-day ransomware and all known physical and remote access attacks.

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.

Zero Trust File Acess

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

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

Dual Mode

Not FIPS 140-2 Validated

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 internerationally without concern of data loss. Create a secret, secure drive that adversaires 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.

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.

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.

To put Cigent to the test, multiple teams of the world's leading experts in advanced data recovery used all known classified and unclassified techniques, tactics, and procedures to attempt to access data protected by Cigent and were unsuccessful.

CIGENT PLUS

Optional
Software as a Service Add-on

Enterprise-wide data security includes secure file sharing and Cigent Secure SSD management enabling customizable security controls and integration with existing security solutions.

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
- Work from home increases the risk of adversaries gaining physical access to the device

Enhanced Security Capabilities

- Enterprise Digital Rights Management
- Enterprise auth factors
- Integration with NGAV and EDR
- Advanced risk-based threat detection
- RESTful APIs for SIEM integration

Enterprise Management Console

- Multi-tenant, hosted or on-prem
- Group policy settings
- Threat and event reporting
- Notifications
- File encryption key recovery

Cigent Secure SSD Advanced Technical Specifications

Technical Specs

- Capacities: 512GB, 1TB, 2TB, 4TB†
- OS: Microsoft Windows® 7, 8, 10, 11
- Available as internal M.2 2280 or external
- USB 3.0/USB-C Adapter and Cable
- 3D TLC NAND Flash Memory
- PCIe Gen3x4 NVMe 1.3 Interface
- Maximum Sequential Read Speed: 3200 MBps
- Maximum Sequential Write Speed: 1000 MBps
- Maximum Random Read Speed: 200K IOPS
- Maximum Random Write Speed: 20KL IOPS
- Maximum USB Transfer Rate: 625 MBps
- TCG Opal 2.0 Encryption

†Not available as FIPS 140-2 Validated

Certifications

- FIPS 140-2 Level 2 Validated
- TAA Compliant

Operation

- Power: 3.3V+/- 5%
- Operating Temp: 0°C to +70°C
- Storage Temp: -40°C to +85°C
- 12-Month Hardware Warranty

Dimensions (Excluding Case)

- 80 mm (l) x 22 mm (w) x 35 mm (h)

Inquiries

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

Email:
General Inquiries - info@cigent.com
Sales Inquiries - sales@cigent.com
Partner Inquiries - 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