CIGENT

CIGENT SECURE SSD PREMIUM

DATA SHEET v1.1

PROUDLY FUNDED BY

iqt IN-Q-TEL

The Most Secure Storage Available

Self-defending SSD with a dedicated security microprocessor, disconnection detection switch, accelerometer, and capacitors automatically defeats attacks.

- Invisible data
- Hacker-proof credentials
- Keep-alive heartbeat
- Verified data destruction
- Secure access logs
- Zero trust file access
- Emebedded ransomware detection
- Disconnect detection and response
- Wipe, clone, alt O/S boot prevention
- Emergency automated wipe
- Movement detection and response
- Dual mode

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's mission is to address advanced cyber threats by moving from a reactionary detect and respond approach to protecting the data itself with invisible, zero trust data protection that is unassailable to even the most sophisticated adversaries who have physical or remote device access.

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

Disconnect Detection and Reponse

Physical circuit on the SSD connector triggers an automated response when the SSD is removed from the PC or external case.

- Emergency automated wipe once drive is connected to power again
- Capacitors on SSD maintain battery life when disconnected enabling automated response even when disconnected from power

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

Wipe, Clone, Alt O/S Boot Prevention

Non-bypassable AI running on dedicated security microprocessor on SSD monitors for nefarious activity and automatically prevents data compromise.

- AI based on data access patterns sees any attempt to wipe drive, clone drive, or boot PC from an alternate O/S
- Also prevents adversaries from removing drive from PC and plugging into another system to try to access data

Dual Mode

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

- Create a secret and secure drive that adversaries cannot know exists
- Travel internationally without concern of data loss
- Enable corporate and personal use without risk of compromise

Emergency Automated Wipe

Embedded full drive NVME Secure Erasure with Verified Data Destruction.

- Triggerable by movement detection, drive removal, application, or command line interface
- Significantly safer, easier, and more reliable approach to full drive erasure for emergency data destruction checklists

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.

CIGENT CAPABILITIES

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.

Movement Detection and Response

Programmable accelerometer on SSD detects movement patterns and enables multiple automated responses including locking drive, wiping drive, and flipping Dual Mode sides.

- Enables simple, effective, and reliable emergency automated wipe scenarios for emergency destruction checklists
- SSD can be set to switch to dual mode "cleared" side as automated response to specific movement patterns

Verified Data Destruction

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

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

Embedded Ransomware Detection

Industry's only embedded ransomware machine learning on dedicated security microprocessor automatically responds to zero day ransomware.

- Automated response includes locking drive partitions or making them read-only
- Ransomware machine learning detection based on non-bypassable storage data access I/O patterns consistently detecting zero days

Keep-alive Heartbeat

Independent file filter driver and firmware heartbeats that prevent file access if Cigent software is disabled.

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

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

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

What makes Cigent so effective?

- Our protection begins in storage firmware.
- We protect the data itself vs. the device or network.
- We make data invisible.
- Our credentials cannot be accessed.

CIGENT PLUS

Optional
Software as a Service Add-on

Enterprise-wide Cigent Secure SSD management enabling customizable security controls and integration with existing security solutions.

Enhanced Security Capabilities

- 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

Cigent Secure SSD Premium Technical Specifications

12-Month Hardware Warranty

Technical Specs & Certifications

- Capacities: 512GB, 1TB, 2TB 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/Write 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
- TAA Compliant

Operation

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

Dimensions (Excluding Case)

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

O/S Support

- Linux and Windows set-up utility
- Once configured, SSD will self-defend on any O/S
- Optional Windows Zero Trust File Access software

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.