CIGENT

CIGENT SECURE SSD

Data Sheet

FIPS VALIDATED 140-2

PROUDLY FUNDED BY

iqt IN-Q-TEL

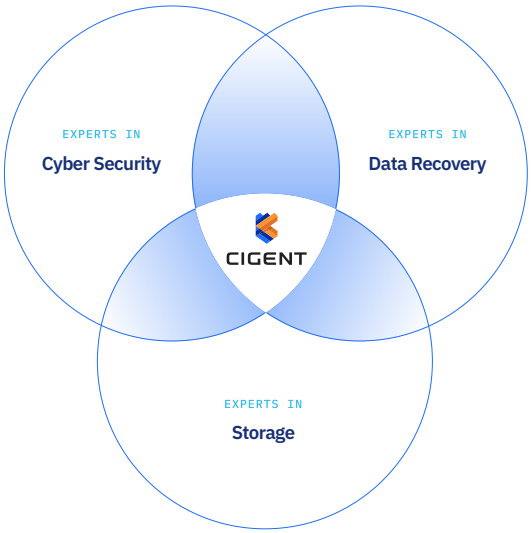
Next Gen Data Protection

The most secure place to store data is now the edge.

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 recovery, 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 recovery, 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. Edge devices like endpoints have and will always contain sensitive data and need to be protected from data theft 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 protect the data itself vs. the device or network
- ✓ We make data invisible protected by non-recoverable keys
- ✓ We protect visible data with MFA for file access

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™

Government-certified Data at Rest Protection

Government-certified Data at Rest (DAR) protection that complies with FIPS, CC, and CSfC, protecting data on any O/S with full disk encryption, MFA, crypto erase, verified full drive erasure and on Windows OS makes data invisible, automatically responds to threats, and has immutable insider detection.

Invisible Data: **Adversaries cannot steal what they cannot see: unreadable storage partition protected by non-recoverable key**

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.

Non-Recoverable Keys: **A novel approach to the creation and storage of keys that prevents all known key recovery techniques**

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

MFA for File Access: **Zero-day ransomware, malware, and software service bypass prevention**

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

Automated Threat Response: **Makes data invisible if Cigent software is disabled**

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

Verified Device Erasure: **Ensures every block has truly been wiped**

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

Immutable Insider Detection: **Secure data access logs capture all insider threat activity**

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, MITRE and 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.

ARCHITECTURE STACK

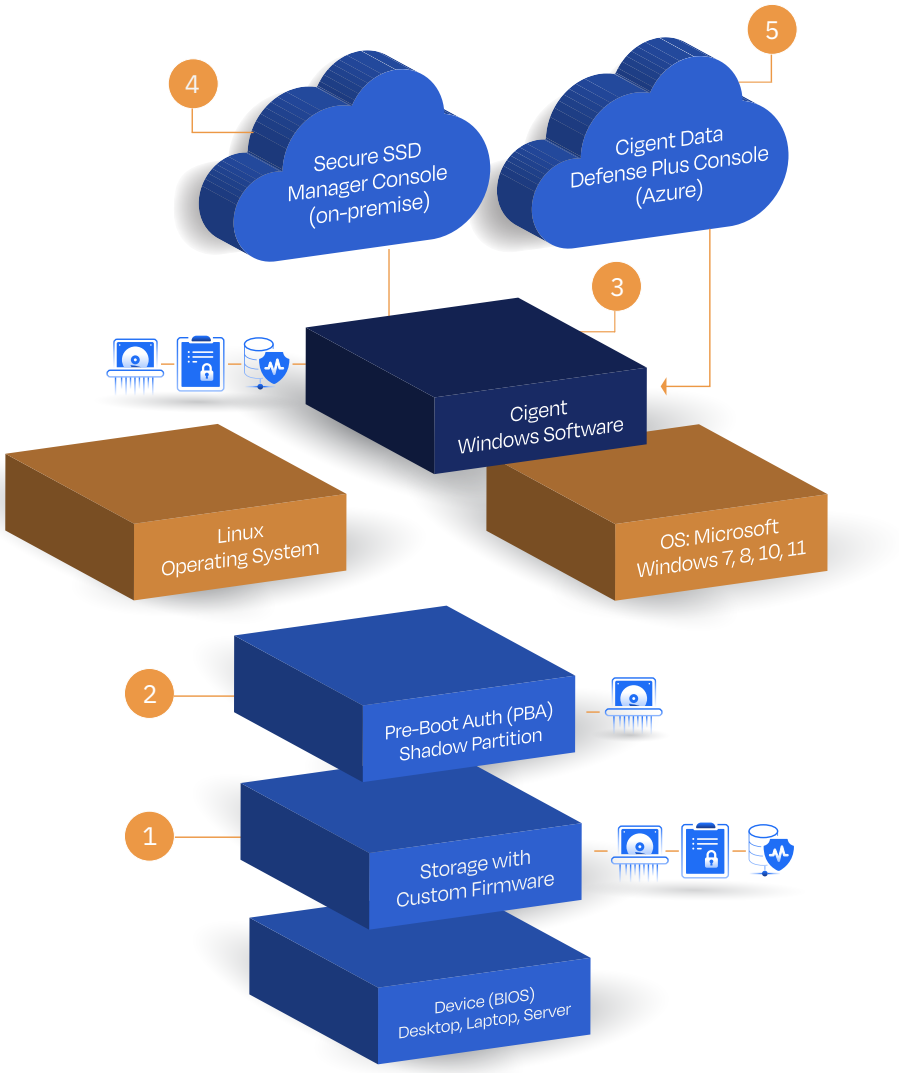
5 Cigent Data Defense Plus Console (Azure)
– All capabilities of Cigent Secure SSD Manager Console (on-premise) plus:
- Digital Rights Management*
- File Encryption*
- Secure File Sharing*

4 Cigent Secure SSD Manager Console (on-premise):
– Windows Software:
– User/Group Policy Setting
– Integration with SIEM and EDR tools
– Threat and Event History and Notifications
– User Key and PIN Recovery

3 Cigent Windows Software:
– Invisible Data
– MFA for File Access
– Verified Device Erasure
– Automated Threat Response
– Immutable Insider Detection

2 Pre-Boot Auth (PBA) Shadow Partition:
– O/S agnostic Full Disk Encryption
– Pre boot auth with password, CAC/PIV, or both for MFA
– Crypto Erase
– Full NVMe Drive Erasure Verified by Firmware Based Verified Device Erasure

1 Firmware-level capabilities built-in to the storage device:
– Automated Threat Response*
– Verified Device Erasure
– Immutable Insider Detection*



* Cigent Windows Software required

Automated Threat Response | Immutable Insider Detection | Verified Device Erasure

CIGENT SECURE SSD

Cigent Secure SSD data protection is available from Cigent and our Cigent Secure SSD Ready partners Kanguru, DIGISTOR, and Seagate.

Technical Specs	Cigent		Kanguru	DIGISTOR	Seagate
Product	Cigent Secure SSD	Cigent Secure SSD FIPS	Defender SED300	Citadel C Series Advanced	Barracuda 515
Capacities / Part Numbers					
256GB	CGN-110020I	N/A	TBA	DIG-M2N2C22566	ZP256MC300212
512GB	CGN-110050I	CGN-110050IF	TBA	DIG-M2N2C25126	ZP512MC300212
1TB	CGN-110100I	CGN-110100IF	TBA	DIG-M2N2C210006	ZP1024C300212
2TB	CGN-110200I	CGN-110200IF	TBA	DIG-M2N2C220006	ZP2048C300212
4TB†	CGN-110400I	N/A	TBA	N/A	N/A
3D TLC NAND Flash Memory Operation	✓	✓	✓	✓	✓
PCie Gen3x4 NVMe M.2 2280 1.3 Interface	✓	✓	✓	✓	✓
Maximum Sequential Read Speed: 3200 MBps	✓	✓	✓	✓	✓
Maximum Sequential Write Speed: 1000 MBps	✓	✓	✓	✓	✓
Maximum Random Read Speed: 200K IOPS	✓	✓	✓	✓	✓
Maximum USB Transfer Rate: 625 MBps	✓	✓	✓	✓	✓
AES-256 RSA-2048 TCG Opal 2.0 Encryption	✓	✓	✓	✓	✓
Certifications					
TAA Compliant	✓	✓	✓	✓	✓
NIST FIPS 140-2 Level 2 Validated	N/A	4186	4295	4294	4294
NIAP Common Criteria FDE_EE	N/A	N/A	N/A	VID 11297	VID 11322
NIAP Common Criteria FDE_AA	PENDING	PENDING	N/A	PENDING	PENDING
NSA CSfC DAR Capabilities Package 5.0	N/A	N/A	N/A	COMPLIANT	COMPLIANT
Operation					
Power: 3.3V+/- 5%	✓	✓	✓	✓	✓
Operating Temp: 0°C to +70°C	✓	✓	✓	✓	✓
Storage Temp: -40°C to +85°C	✓	✓	✓	✓	✓
Warranty					
Hardware Warranty	1 YEAR	1 YEAR	TBA	3 YEARS	5 YEARS
Software Warranty	1 YEAR	1 YEAR	1 YEAR	1 YEAR	1 YEAR
Dimensions					
80 mm (l) x 22 mm (w) x 35 mm (h)	✓	✓	✓	✓	✓
Add-ons					
Cigent Secure SSD Manager License (Includes 5 Years of Software Support and Updates)					
Cigent Data Defense Plus					
Cigent External USB Case with USB 3.0/USB Cable					
Rugged Removable Format (available from DIGISTOR for Citadel C Series Advanced SSDs)					

Features and Capabilities

Feature	Cigent Secure SSD
SATA Operation Support	AHCI
Pre-Boot Authentication (PBA)	✓
PBA Authorization Factors	Password, CAC/PIV smartcard
Languages	English
Crypto Erase	✓
Erase Disk	✓
Change Authentication Keys	✓
Activity Log	✓
Mass Deployment Support	✓
Failed Logins Before Lockout	✓
Failed Logins Before Disk Erase	✓
Password History	✓
Database Backup	✓
Install and Update Integrity Validation	✓
Password Complexity Options	Always requires 4 character types
Two-Factor Authentication	✓
Unreadable storage partition protected by non-recoverable key	✓
Verified Device Erasure	✓
Immutable Insider Detection	✓
Automated Threat Response	✓

Achieve Compliance With

Regulation	Summary
FAR	Federal Acquisition Regulation
DFARS	Defense Federal Acquisition Regulation
TAA	Trade Agreements Act – Designates countries products can be bought from
FIPS 140-2 Level 2	Security requirements that must be met by cryptographic (encryption) modules
NIAP Common Criteria FDE_EE and FDE_AA (pending)	USG protection profile for Full Drive Encryption
HIPAA	Health Insurance Portability and Accountability Act of 1996
GDPR	General Data Protection Regulation (EU GDPR)
CCPA	California Consumer Privacy Act of 2018
GLBA	The Gramm-Leach-Bliley Act
CSfC DAR Capability Package 5.0	NSA Commercial Solutions for Classified (CSfC) policy for Data at Rest (DAR)
NIST 800-171	Protecting Controlled Unclassified Information (CIU) on Nonfederal Systems
CMMC (Levels 1-5)	Cybersecurity Maturity Model Certification
Executive Order (EO) 14028 May 12, 2021	Presidential order to all USG agencies for Improving the Nation's Cyber Security

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

©2022 Cigent Technology Inc. All rights reserved.

Cigent is a registered trademark and Secure SSD and Impossibly Secure are trademarks of Cigent Technology Inc. In the United States and other jurisdictions. SS20210823