
CIGENT
Protect your data from any threat vector
even after a security breach.

For Three Decades, the Industry Has Consistently Failed to Prevent Ransomware and Data Theft.

- Software-only security layers have inherent vulnerabilities
- Unlimited number of ever-evolving threat vectors

Data unencrypted after login	Personal or BYOD PCs	Vulnerabilities
Once a user logs into their PC, whether in use or idle, the PC is accessible to adversary.	Insufficient security protections. Sensitive files being saved.	Myriad known software vulnerabilities, often unpatched or months to patch. Multitude unknown vulnerabilities.
Unhealthy PC state	**Advanced/fileless attacks**	**Credential compromise**
Configuration drift, agent corruption, OS updates, security app conflicts, etc.	Advanced malware able to bypass NGAV, fileless malware and live off the land attacks not detected in time.	Credential theft, poor hygiene and password management enables easy access to system/data.
Supply Chain/APTs	**Disabled Security Software**	**Malicious Insiders**
Supply chain attacks, chip implants, BIOS and firmware malware and vulnerabilities, bootkits/rootkits, etc.	Advanced attackers disable security software and protections.	Able to exfiltrate data from their own PCs undetected and move laterally to other PCs for data exfiltration.

An entirely new approach: Assume there will be a security breach and protect the data.

- Zero Trust file access controls at the data level that rely on multi-factor authentication to defend against data theft and ransomware, even if the system is compromised.
- Protects data at the endpoint, on the network, in the cloud, or when shared with trusted users
- First and only family of self-defending storage devices with cybersecurity placed as close to the data as possible – into the firmware itself
- Dedicated security processor uses machine learning to detect & respond to ransomware attacks
- Protects sensitive files at all times from any threat vector, even in post-breach environments

Cigent Data Defense

CIGENT

Cigent Is…

A fusion of the best experts in storage, data recovery, and cyber security with an In-Q-Tel-backed mission to commercialize its government/military-grade technology which defends businesses and individuals from inevitable security breaches, by protecting the data itself from any threat vector.

CIGENT

Protecting your data from the inside out

Expertise in Data and Network Security

- 35+ years cyber / data security experience
- Roots in advanced data destruction and recovery
- Worked with government agencies on technology solutions
- National Scientific Achievement Award for technology innovations in data security to co-founder
- 24/7/365 SOC (soon to be type 2 certified)
- Curating all govt open-source databases of cyber intel
- InfraGard member

Solid Funding and Advisors

- Series A complete
- VCs: In-Q-Tel, CyberJunction, WestWave Capital
- Investors /senior advisors include:
  - Avie Tevanian
    (Former Apple Chief Software Technology Officer)
  - Tom Paquin
    (Mozilla and Netscape Co-Founder)
  - Tom DiBenedetto
    (CyberJunction Founder, Fenway Sports Group Partner, Chairman of Jefferson Waterman Intl.)

Ground-Breaking, Proven Technology

- 100% own I.P.; 5 issued patents; 15 pending
- Government-proven technology now available for enterprise use
- Industry first approach to always protect sensitive files from any threat vector, before or after a security breach.
- First & only family of self-defending storage devices with cybersecurity built into the firmware

Leading Cyber Security Partner Alliances

- **OS**: Microsoft Windows 7/10, Windows 10 Hello
- **Cyber**: CyberArk, Microsoft Windows 10 Security, PC Matic, Sophos, VMware Carbon Black, Cisco Secure Endpoint
- **Channel**: Dell, Optiv, Immix Group, Staples

Cigent Data Defense Solutions:

Product Overview

CIGENT

It Starts With Software: Cigent **D3E** for Windows

D3E – The Agent For Cigent Data Defense

Zero-Trust file access controls rely on multi-factor authentication to defend against data theft and ransomware, even if the system is compromised, and allow both individuals and organizations to easily encrypt and control access to sensitive files so that they can be securely stored in any location and shared with trusted users. Use with/without Secure SSDs.

Hero features

- **ActiveLock**
- **Multi-factor Authentication**
- **Posture Based**
- **Threat Sensor Platform**
- **3rd Party Integrations**
- **Management Console**
- **Everywhere Features**

Fingerprint

Via Windows Hello

Facial Recognition

Via Windows Hello

PIN

Personal Identification Number

Authenticator Apps

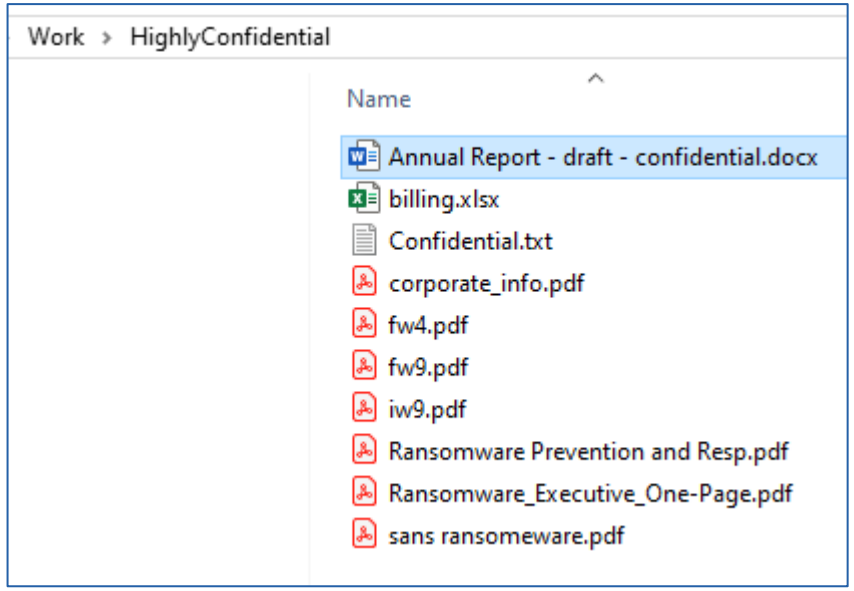
Time-based one-time password

Duo Security

Time-based one-time password and push

CIGENT

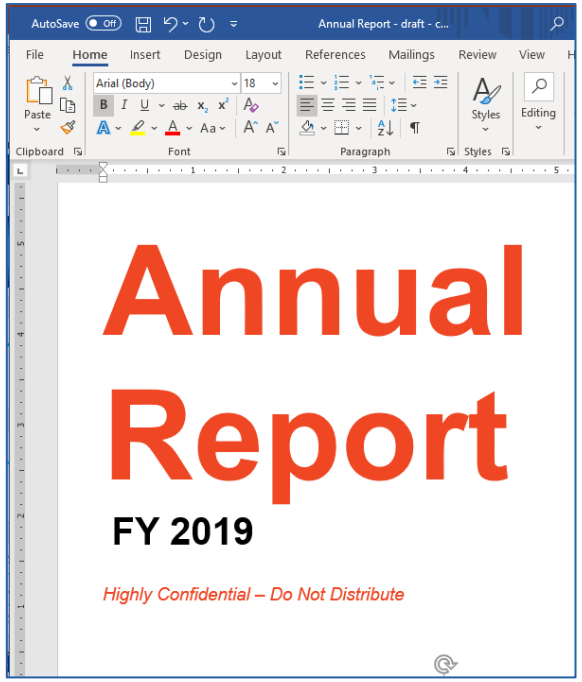
Simple, nondisruptive but extremely effective file protection



Ransomware

Vengeful Insiders

Compromised Credentials



Open Sensitive file as usual

Touch Fingerprint reader

File Opens

CIGENT

Data Defense Hardware: Cigent **Secure** SSD

Cigent Secure SSDs - K2 / Denali

Self-defending storage devices with cybersecurity built into the firmware itself with a dedicated security AI processor that detects and respond to ransomware, a keep-alive sensor that automatically encrypts sensitive files if security software is bypassed, and a safe room that makes data invisible to any attacker.

Hero features

- **Secure Drive** | "safe room"
- **Log Auditing** | hardware-protected
- **Keep Alive** | security software heartbeat
- **True Erase** | drive erasure verification
- **Ransomware** | ML-based ransomware detection
- **Dual Mode** | flip mode - dual hidden drives

Three configs (TCG Opal 2.0)

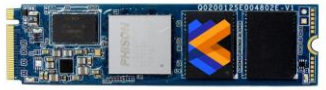
- NVME M.2 Internal SSD
- SATA M.2 ½" Internal SSD
- USB External SSD

Capacities

- 512GB, 1TB, 2TB

CIGENT

Cigent **Denali** – Embedded Ransomware Detection



Secure Drive
Log Auditing
Keep Alive
True Erase
Ransomware
Dual Mode

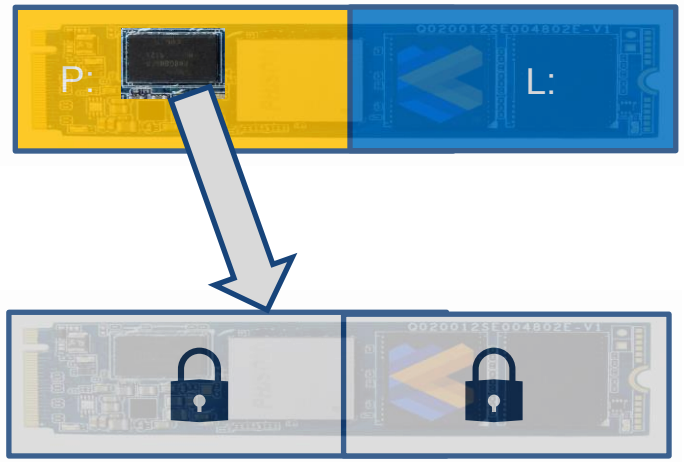
Firmware-Based Ransomware Protection

- AI-driven ransomware detection and defense in real-time directly in the storage itself
- Self-defending device, does not need OS or software
- "Safe Room" makes data disappear during the threat, but remains accessible by authenticated users

Benefits

- Removes access to the one thing ransomware attacks need – your data
- Lost/stolen computers, insider access to computers, no problem
- Does not rely on an operating system or software, so will protect data even when all systems are breached

Security Chip analyzes data in real-time



CIGENT

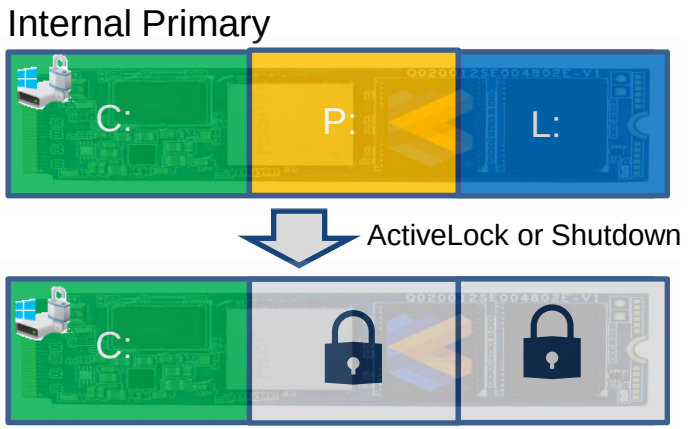
Cigent **Secure** SSD storage – Secure Drive

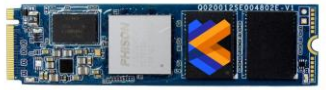
Secure Drive

- Data protected using AES-256bit encryption
- TCG Opal 2.0 range locking protects partitions(drives) from authorized access
- DYNAMIC – Authentication required during elevated threat state
- ALWAYS-ON – Authentication ALWAYS required
- Device sharing possible with password and D3E authentication
- Bitlocker unprotected and Cigent partitions

Benefit

- Data secure at rest AND in use (with D3E)



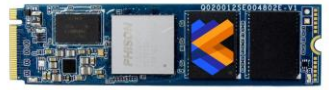


Secure Drive
Log Auditing
Keep Alive
True Erase
Ransomware
Dual Mode

Unprotected
Dynamic
Always On

CIGENT

Cigent **Secure** SSD storage – Command Log Audit



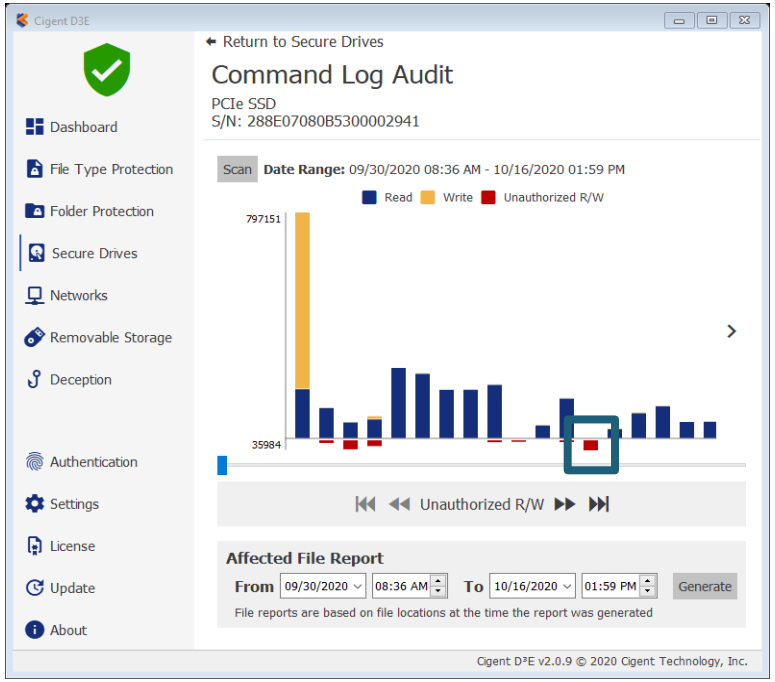
Secure Drive
Log Auditing
Keep Alive
True Erase
Ransomware
Dual Mode

Command Log Audit

- Metadata for every command sent to log is stored in firmware memory for later analysis
- Agent(D3E) markers in log used to determine authorized attempts to access drive/data
- Generate report of 'affected files' based on current filesystem.

Benefit

- Capture unauthorized attempts to access drive
- Reduce scope of breaches



Unauthorized access

Cigent **Secure** SSD storage – Keep Alive

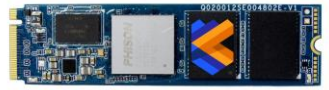
Keep Alive

- Periodic non-replayable sequence between OS agent(D3E) and firmware
- Tethers SSD to agent
- Missed heartbeat response – Drive locks

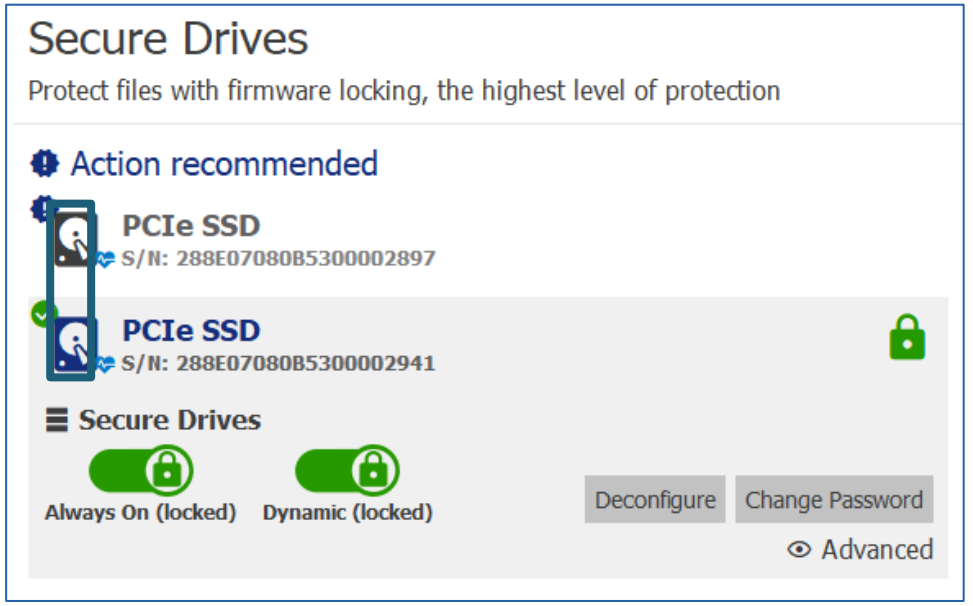
Benefit

- Ensures authentication for drive and file access cannot be bypassed

KeepAlive - Enabled



Secure Drive
Log Auditing
Keep Alive
True Erase
Ransomware
Dual Mode



Cigent **Secure** SSD storage – True Erase

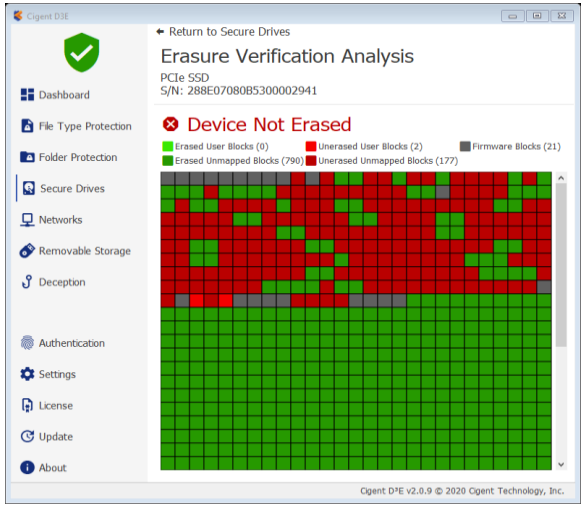
True Erase

- Block level verification that all data has been securely destroyed.
- Verify step in Secure Data Destruction procedure

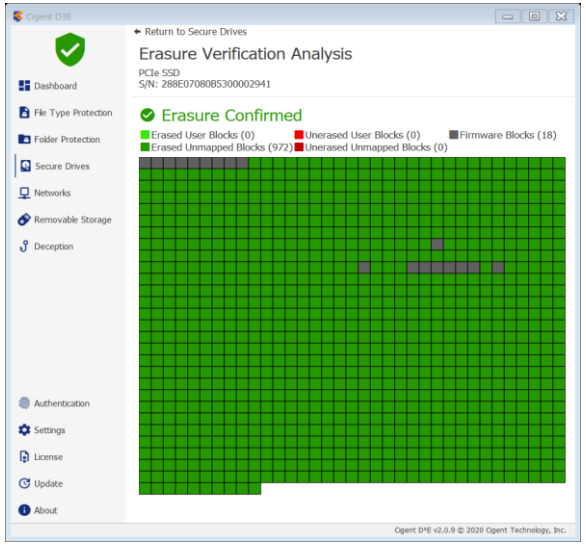
  ie nvme format /dev/nvme0 –namespace-id=1 –ses=1

Benefit

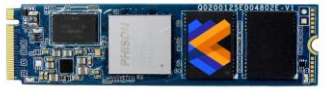
- Safely repurpose SSD/laptop – Increase ROI



User data persists

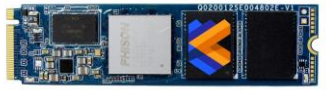


All data erased



Secure Drive
Log Auditing
Keep Alive
True Erase
Ransomware
Dual Mode

Cigent **Denali** – Dual Mode

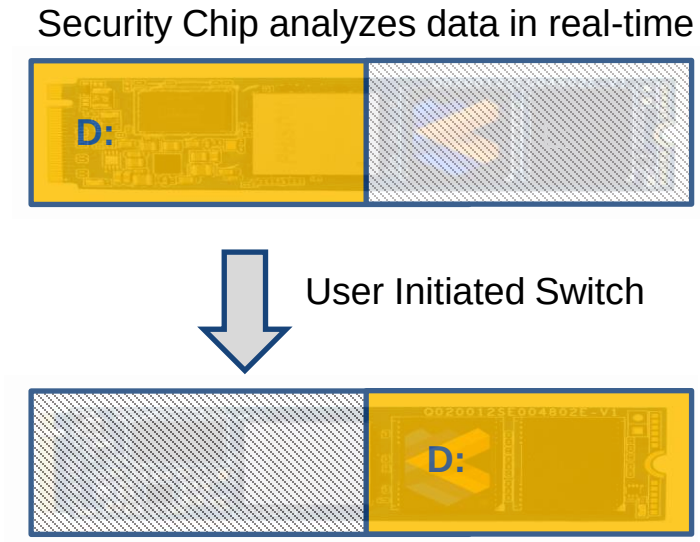


Dual Mode

- "Safe room" that makes data invisible to attackers
- Mutually-exclusive active partitions
- Lets you work in a hidden secure drive
- Cigent software and password required to switch

Benefits

- Completely hide sensitive data even if system examined by knowledgeable attacker
- Optionally require conditions before swapping (i.e. attached to secure network)



Appendix

Sensors - Raise the Threat Level

State

Network

USB storage

AV endpoint

External Integrations

Windows Defender

PC Matic

VMware Carbon Black

Cisco Secure Endpoint

CyberArk

Sophos

Deception

File and network honeypots

Artificial Intelligence

File I/O pattern

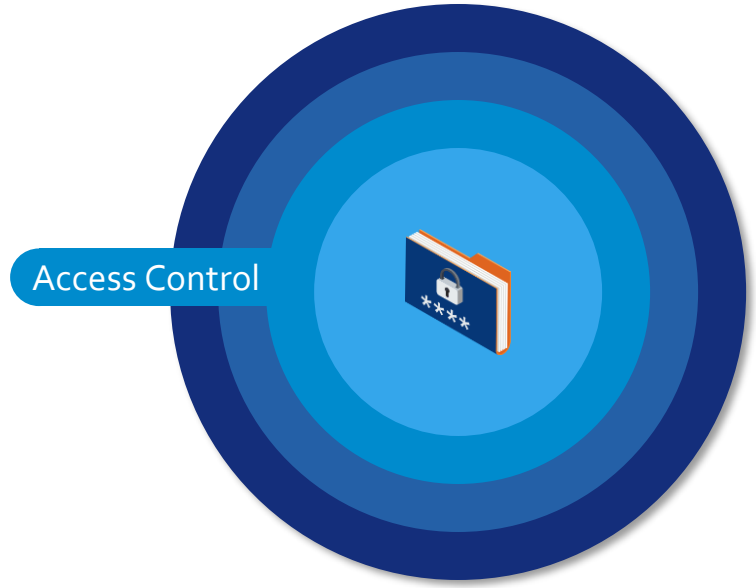
Keyboard typing pattern

User access pattern

Access Control

- Powered by Active Lock
- Posture-based step-up authentication for file access

Designation	Posture	
	Normal	Elevated
Always On	Authorization Req.	Authorization Req.
Dynamic	No Authorization	Authorization Req.



CIGENT