SNIA STORAGE SECURITY SUMMIT

Wednesday, May 11, 2022 • Virtual

Storage with Embedded Cybersecurity to Truly Protect Data

Tom Ricoy, Vice President of Strategic Alliances, **Cigent Technology Inc.**

snia.org/storage-security-summit

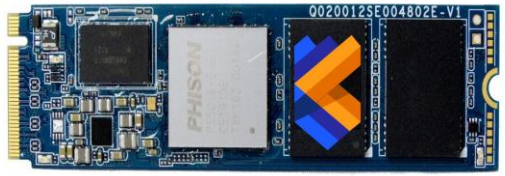
CIGENT

Cigent® renders your data invisible. Attackers cannot compromise what they cannot see.

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.

STORAGE WITH EMBEDDED CYBER SECURITY ARCHITECTURE

Hardware



- SSD (Self encrypting drive with hardware encryption)
- Standard firmware code
- Custom additional firmware code
- Cyber security chip
- Accelerometer, disconnect detection circuit, additional capacitors

Software

CIGENT

- Endpoint Agent
- Management Console

STORAGE AND SOFTWARE WORK IN TANDEM

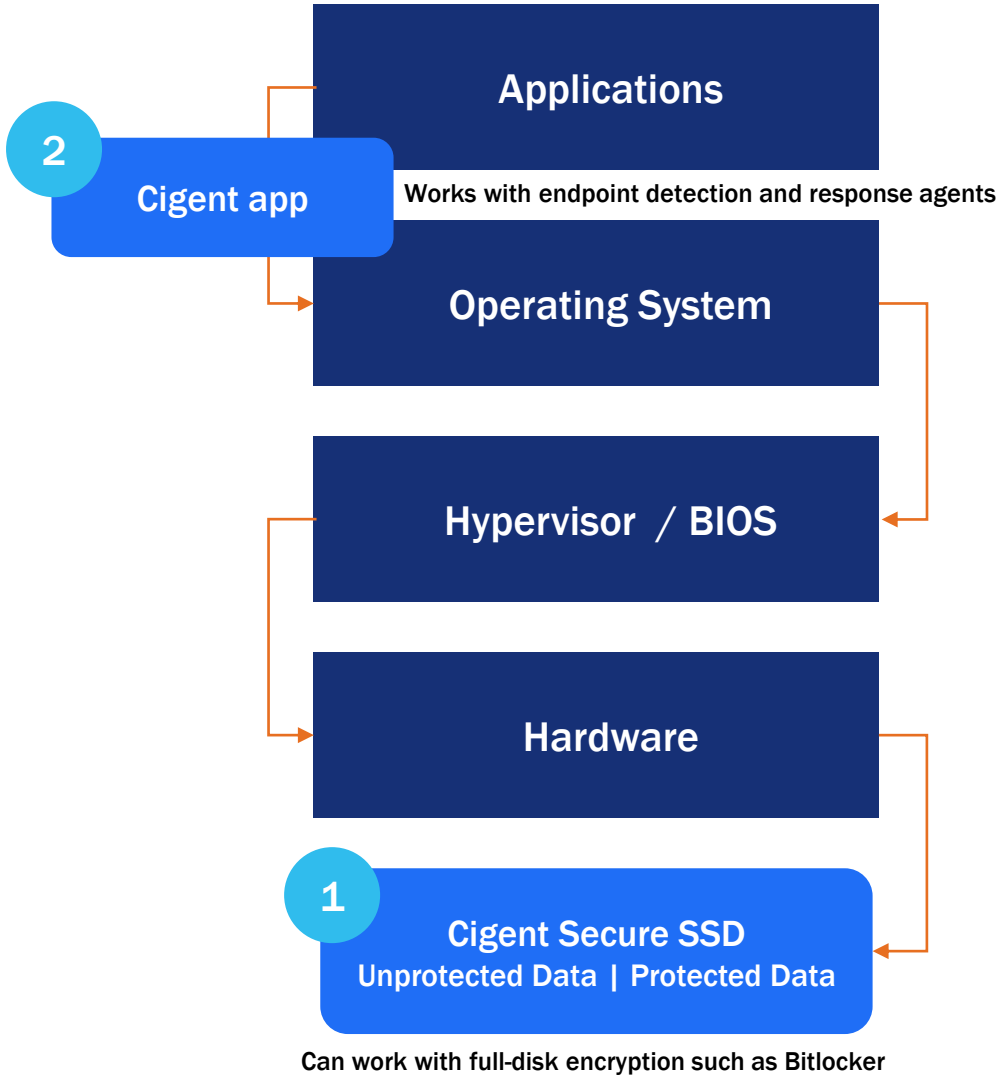
Cigent Solution

1. Cigent Secure SSD™ creates a secure partition for confidential data
2. Cigent app provides file-level encryption and file access controls

User logs into Windows, data remains invisible until unlocked with MFA

Secure partitions and file access controls can be configured for:

- Zero-trust – MFA always required to unlock partition and access files
- Risk-based – MFA only required during elevated threat state



KEY SECURITY CHALLENGES ADDRESSED

Protect endpoint data when a device has been lost, stolen, or confiscated	**Cigent stops physical access attacks**
Protect endpoint data from loss after drive wipes that fail to erase all data	**Cigent verifies data destruction**
Protect endpoint data from remote attacks like ransomware and disabling EDR	**Cigent defeats remote data attacks**

CIGENT

Lost, stolen, or confiscated devices present unique security challenges

- 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 risk of adversaries gaining physical access to devices

Physical Attacks

Software full-disk encryption (FDE) and self-encrypting drive (SED) protections can be defeated by adversaries who have physical device access

REMOTE ATTACK CHALLENGES

Approach is dependent upon detecting threats before they can execute

- 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

Remote Attacks

Advanced malware, fileless malware, living-off-the-land, zero-day, supply chain, and social engineering attacks able to bypass EDR

FUNDAMENTAL SECURE STORAGE CAPABILITIES

Invisible Data

Data is invisible, even after logging on

- 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

Tamper-proof Credentials

Makes credential access impossible

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

PROTECTING DATA WHEN SECURITY SOFTWARE IS DISABLED

Keep-alive Heartbeat

Storage firmware heartbeat ensures Cigent software is always running

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

Zero Trust File Access

Only trusted user can access files

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

FIRMWARE-LEVEL STORAGE SECURITY CAPABILITIES

CIGENT

Verified Data Destruction

Block-level verification that data is irrevocably deleted and unretrievable

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

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

Dual Mode

Two drives on a single SSD with unique O/S’ invisible at the BIOS level

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

HARDWARE ENHANCED SECURITY CAPABILITIES

CIGENT

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

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

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

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

Tom Ricoy - Tom.Ricoy@cigent.com