CIGENT

COMPANY PROFILE

IMPOSSIBLY SECURE | | 2022

SUMMARY

Cyberattacks and data breaches are inevitable. Keeping data secure seems impossible. Hackers employ various tactics to compromise endpoint devices to access your data. Current protections will continue to be defeated, leaving data vulnerable to compromise. Just one vulnerability opens the door for a physical or remote attack to occur.

Endpoint devices are vulnerable to physical attacks when lost, stolen, confiscated, or compromised by remote access. Existing protections, including full disk encryption (FDE), self-encrypting drives (SEDs), and endpoint detection and response (EDR), have failed to protect data. Files are stored in multiple locations and shared with others making them easily accessible to adversaries. Data Loss Prevention (DLP) solutions are complex to manage and too restrictive for users.

Cigent® protects your most valuable asset – your data – with Cigent Secure SSDs™ that prevent compromise by attackers who gain remote or physical access to a device and zero trust access controls that protect individual files wherever they go.

Our Story

Cigent co-founder John Benkert spent 20 years in USAF Intelligence and seven in the NSA where he received the National Scientific Achievement Award for technological innovations in data security. He is the owner of CPR Tools, leading experts in data recovery, forensics, and destruction since 1987.

Recognizing the vulnerabilities in data security solutions including FDE and SEDs, Benkert set out to design a more secure approach to data protection - one that could not be defeated no matter the situation or adversary. He formed a team of experts in storage, data forensics, and cyber security.

Securing funding from In-Q-Tel, the Cigent team has achieved Benkert's vision of developing the most secure data security solution available.

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.

Physical Attacks

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.

Software encryption like Bitlocker is easily compromised utilizing a variety of methods. Attackers often start by probing for weak credentials and leveraging commercially available tools like passware kits. If this fails, they generally employ kernel or rootkit attacks or alter or manipulate the O/S, thus allowing encryption keys to be accessed. Even unsophisticated adversaries can usually defeat software FDE solutions and access or steal your confidential data.

While SEDs provide elevated protection, they are also vulnerable to more sophisticated but well-established approaches. Assailants often utilize tools such as WinHex and R-Studio to identify configuration

failures. They also use brute force attacks, chip-off, and reverse engineering of the firmware. If those approaches prove unsuccessful, attackers may utilize direct physical attacks, including x-ray examinations and chip dumps. In summary, SEDs provide better protection than software FDE but can and will be defeated by a motivated attacker, thus exposing your confidential data.

Remote Attacks

Data compromise also occurs from remote attacks. Despite billions invested in EDR and other endpoint protection software, compromises continue to accelerate in number and severity. Each year sets new records for successful ransomware exploits and payments. Attackers continue to find success due to:

- Ability to disable endpoint security software
- Vast number of unpatched known and unknown software vulnerabilities
- Sophisticated attackers utilizing increasingly specialized tactics and capabilities
- Supply chain and firmware attacks

Attackers exploit vulnerabilities to infect devices, systematically compromise the environment, and execute their objective, including exfiltration, modification, or encryption. An attacker only has to succeed once to compromise all your data.

Data Loss

DLP is complex to manage and too restrictive on users. Organizations cannot control access to files when stored on clouds, collaboration platforms, emailed outside the company or saved to removable media, making them easily accessible to adversaries.

- Adversaries who compromise user credentials, clouds, hosted apps, or email can get access to an organization's data
- Data Loss Prevention (DLP) solutions are complex to implement, manage, maintain, and bog down security teams with many notifications without context
- Application-specific Rights Management Systems (RMS) only provide data protection for specific file types
- Data protection solutions that prevent employees from doing their job create shadow IT and resentment for security policies

How can you protect your endpoint data from the seemingly inevitable compromise?

INTRODUCING CIGENT

Data secured by Cigent cannot be hacked, ransomed, stolen or exfiltrated as it remains invisible to unauthorized parties protected by tamper-proof credentials and the industry's only zero-trust file level security.

PROUDLY FUNDED BY

iqt IN-Q-TEL™

Cigent is Impossibly Secure™

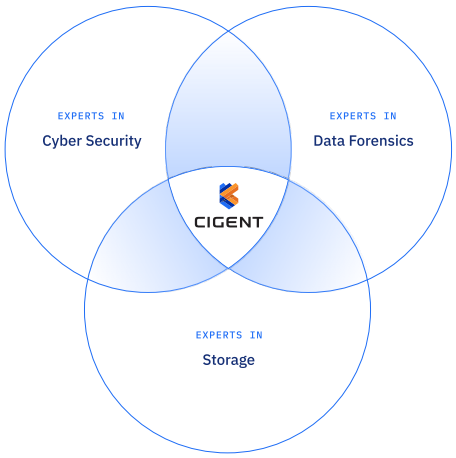
Render your data invisible. Attackers cannot compromise what they cannot see.

Our Solution

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. Wherever files secured by Cigent go, they cannot be accessed by unauthorized users as the data remains encrypted, protected by digital rights management and the industry's only zero trust file access security.

Our Product

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.

Stop Ransomware and Remote Attacks

Prevent remote attackers who have overcome EDR from compromising or even viewing Cigent protected data.

Invisible Data

Data is unreadable at the sector level even after logging on until unlocked with MFA and automatically hides again when the user locks the screen.

Zero Trust File Access

File access controls block zero-day ransomware and only allow the trusted user to access files with MFA.

Keep-alive Heartbeat

Storage firmware heartbeat ensures Cigent software is always running and makes in-use data invisible if attackers disable Cigent software.

Stop Physical Data Exfiltration

Prevent data compromise when a device has been lost, stolen, or confiscated.

Invisible Data

Data is unreadable at the sector level until accessed by the trusted user with MFA.

Tamper-proof Credentials

Credentials are cryptographically derived, never stored in their final form, and use the maximum length, making them inaccessible to adversaries.

Dual Mode

Protected O/S and data are securely stored in a secret drive that cannot be detected, even when storage is viewed with the BIOS.

Protect Data Wherever It Goes

Wherever files secured by Cigent go, they cannot be accessed as the data remains protected.

Secure File Sharing

Files remain encrypted, only accessible by trusted users, wherever they go.

Zero Trust File Access

File access controls only allow trusted users to access files with MFA.

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.

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

Zero Trust File Access

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

- 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

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

Tamper-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

Dual Mode

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 internationally without concern of data loss
- Create a secret, secure drive that adversaries have no way to know is there

Verify 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

CUSTOMER BENEFITS

Your data's confidentiality is secure. Its integrity is secure. Its availability is secure. Sound impossible? It's not. With Cigent.

Secure Your Data with Cigent

Secure your data for confidentiality, integrity, and availability.

Benefits

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

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
- Our credentials cannot be accessed