CIGENT

Put an end to data breaches and ransomware by making data invisiblewith built-in secure storage protected by non-recoverable keys and MFA for file access. Ensure data is only accessed by intended parties when data leaves PC when synced to clouds, cloud apps, emailed, etc. with file encryption and secure file sharing.

CIGENT DATA DEFENSE

DATA SECURITY ON YOUR PC AND WHEREVER IT GOES

CIGENT
DATA DEFENSE

Next Gen Data Protection

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

Stopping Data Breaches and Ransomware Seems Impossible

Adversaries bypass detection and prevention solutions continuously. But they can't compromise what they cannot see.

The answer? Make Your Data Invisible

With Cigent Data Defense, data can literally be made invisible – meaning adversaries cannot see it, much less steal or encrypt it, even if they're using the most advanced data recovery techniques.

Enhance Security with Cigent's Built-In Secure Storage

Most PCs shipp with secure storage with hardware-based encryption for years. With Cigent Data Defense, it can be turned into the most secure place to store data. It is a superior solution to any traditional data protection market offering. Hardware-based encryption is also far more secure than any software-based solution, because software can be corrupted or negated, while hardware cannot. Hardware encryption also has no negative impact on the performance of the system and consistently outperforms software full disk encryption.

Once users make their data visible, CigentData Defense protects designated files with MFA, so your most important data cannot be stolen, ransomed, or compromised.

PROTECT YOUR DATA WHEREVER IT GOES

Today, data does not stay on your PC – it is synced to clouds, stored in cloud apps, collaborated on with colleagues, and shared outside your organization.

With CigentData Defense your data is still safe. Data Defense encrypts your data wherever it goes and ensures only the intended recipients can access it.

For the most comprehensive and secure data protection solution, choose CigentData Defense.

61%

of attacks use **stolen user credentials.**[5]

952M

accounts breached in 2021, an **increase of 31 million** from 2020.[6]

CIGENT

CIGENT DATA DEFENSE

Data protection is having a moment.

70%

of data breaches originate from the **endpoint**.[1]

197 days

Time it takes for most organizations to **detect a data breach**.[3]

$3.9M

The average cost of **a data breach**.[3]

72%

of companies report **malware circumvented** their intrusion detection systems.[2]

4M

Files **are lost every day** due to data exfiltration attacks.[4]

> "Hendry County Schools was pleased to learn of the additional security CigentData Defense offers. With the growing number of ransom-ware attacks targeting schools, we are constantly looking for ways to protect our data that is effective, affordable and easy to implement and manage."

Michael Swindle, Superintendent
Hendry County School District

53%

of executives are **"extremely concerned"** about the effects of cyberthreats on growth prospects.[19]

86%

of businesses that believe in security's ability to open new business opportunities **saw 10%+ revenue growth year** over year.[20]

CIGENT

CIGENT DATA DEFENSE

Protect Data Wherever it Goes

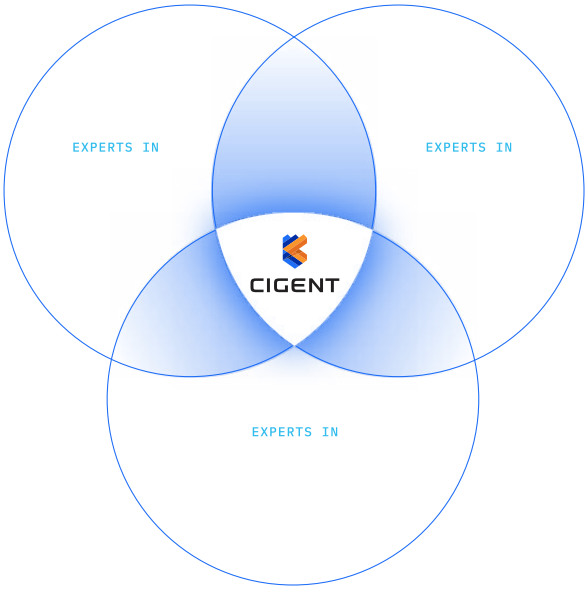
Traditional DLP is complex to manage and too restrictive for users.

Stop Ransomware and Remote Attacks

Advanced adversaries can bypass EDR protections and steal data.

Stop Physical Data Exfiltration

FDE and SEDs can be easily defeated, thus exposing your data when your device is lo confiscated.



CigentData Defense protects your most valuable asset—your data. Using military-grade data security protocols, it protects data against any threat vector.

435%

increase in **ransomware attacks** in 2020.[8]

22 days

average downtime a company experiences after a ransomware event.[9]

CIGENT

CIGENT DATA DEFENSE

A Single Solution with Layered Protections Defending Against All Data Attacks

CigentData Defense protects files from data theft on PCs, clouds, and wherever files go with file encryption and digital rights management, ensuring only trusted users can access files.

Critical files are protected against ransomware and data theft with MFA, and all encrypted files are protected when attacks are detected. Protect against advanced remote and physical access attacks by storing files in an invisible partition that is only accessible by the trusted user with MFA.

MFA for 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

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.

Secure File Sharing

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

- Protect all file types: Office, Adobe, CAD, images, applications – any file
- Users easily share files outside the organization by adding individuals to the file's trusted user list

94%

of organizations have experienced a data breach.[5]

CIGENT

CIGENT DATA DEFENSE

What makes CigentData Defense so effective?

- Embraces zero trust at the file level
- Makes data invisible
- Protects the data itself vs. the device or the network

Customer Benefits

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

Protect files from data theft and ransomware on PCs, clouds, NAS, and wherever files go with file encryption and digital rights management, ensuring only trusted users can access files. Use an Opal SED to protect against advanced remote and physical access attacks.

DATA DEFENSE PLUS FEATURES

Enterprise Management and Enhanced Security

- Enterprise auth factors: Duo Security by Cisco
- Integration with NGAV and EDR: SentinelOne, Cisco Security, Sophos, VMware Carbon Black, CyberARK, PC Matic
- Whitelist apps for cloud syncing, backups, eDiscovery, etc.
- Automated zero trust and risk-based file access and encryption by folder or file type (Office, Adobe, or custom)
- Enterprise Digital Rights Management: enterprise master key to access corporate users' data, file encryption key recovery, deactivate users
- Remotely elevate risk state of endpoints via console (i.e. when SOC determines an eminent threat on user, endpoint, or group)
- RESTful APIs for SIEM integration
- Advanced risk-based threat detection: network/port deception, file deception, new network connections, new removable media insertions

Multi-tenant, hosted or SaaS platform with group policy settings, threat and event reporting, and notifications.

CIGENT

CIGENT DATA DEFENSE

CAPABILITIES	DATA DEFENSE	DATA DEFENSE PLUS
MFA for File Access	Yes	Yes
Invisible Data	Yes	Yes
Secure File Sharing	Yes	Yes
File Encryption	Yes	Yes
ENTERPRISE MANAGEMENT CONSOLE		
Multi-tenant, hosted SaaS platform		Yes
Group Policy Settings		Yes
Threat and Event Reporting		Yes
Notifications		Yes
File Encryption Key Recovery		Yes
ENTERPRISE SECURITY CAPABILITIES		
Enterprise Digital Rights Management		Yes
Enterprise Auth Factors: Duo Security by Cisco		Yes
Integration with NGAV and EDR*		Yes
Advanced Risk-Based Threat Detection		Yes
RESTful APIs for SIEM Integration		Yes
Automated Zero-Trust and Risk-Based Access and Encryption based on Folder or File Type		Yes
Remotely Elevate Risk State of Endpoints		Yes

* Current integrations include: SentinelOne, Cisco Security, Sophos, VMware Carbon Black, CyberARK, PC Matic

CIGENT

SOURCES:

1 https://www.rapid7.com/resources/rapid7-efficient-incident-detection-investigation-saves-money/

2 https://www.forbes.com/sites/theyec/2019/09/18/the-state-of-cybersecurity-pertaining-to-small-business=/?sh 56f3288231a0

3 https://www.ibm.com/security/data-breach

4 https://www.zdnet.com/article/security-what-security-four-million-data-records-are-stolen-or-lost-every-day/

5 https://expertinsights.com/insights/50-identity-and-access-security-stats-you-should-know/

6 https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

7 https://www.pcmag.com/news/united-states-has-the-most-data-breach-victims-in-the-world

8 https://www.digitalinformationworld.com/2022/0l/95- percent-of-cybersecurity-breaches.html

9 https://www.varonis.com/blog/ransomware-statistics-2021

Need Support?

cigent.com

CONNECT

Phone: 669-400-8127
Toll Free: 1-844-256-1825

Email:
info@cigent.com
sales@cigent.com
partners@cigent.com

Headquarters:
2211 Widman Way, Suite 150
Fort Myers, Florida 33901

R&D
402 Amherst St, Suite 402
Nashua, New Hampshire 03063

CIGENT