A New Era of Cyber Resilience
Introducing Fragglestorm©
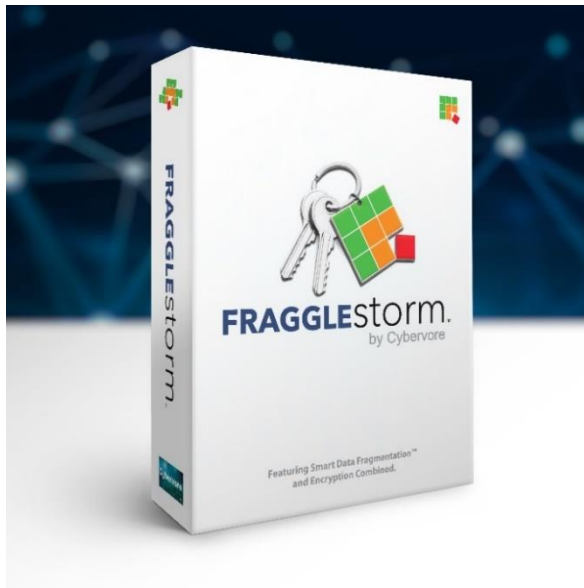
BUILT-IN IDENTITY ACCESS AND MANAGEMENT

Increases Zero-Trust data protection by ensuring only the authorized user can turn on and off their data access, even if the laptop or device is left unattended.

AMPLIFY YOUR DATA PROTECTION

Combines NIST AES 256-bit encryption with fragmentation to store data as unrecognizable smart puzzle pieces.

SIMPLIFY YOUR DATA STORAGE AND SECURITY AT THE SAME TIME

Create a virtual storage drive that protects data immediately, requires no user routine or application changes, and allows only an authenticated user access

- Data breaches are causing irreparable damage to a business's operations and client trust, along with unexpected lawsuits, increased cyber insurance costs, & fines.

- The global average cost of a data breach was $4.45 million. [Source- Ponemon Institute-IBM, 7/23]

- 86% of data breaches involved the use of stolen credentials. It is time to implement strong identity security [Source; 2023 "Data Breach Investigations Report" from Verizon]

- Encrypted or not, stored data does not stop cybercriminals from stealing, extorting, and selling this data because it is valuable.

Data breaches and ransomware have become a major business problem. With secure backups, ransomware recovers. However, once data is stolen, it is likely used for extortion and sold illegally.

Stealing personally identifiable information (PII) and patient health information (PHI) has become a highly sought-after lucrative market across criminal sources and the dark web.

Even if encrypted, this sensitive information is commanding millions in untraceable cryptocurrency payments for its return. Adding Fragglestorm data protection makes unauthorized stolen data worthless and undefinable for resale.

Introducing Fragglestorm™ – Stop the breach by adding stronger security and data privacy protection beyond only using encryption.

Starting at the user endpoint, in transit, and out to cloud storage, Fragglestorm is an easy-to-install, simple-to-use data protection product.

Fragglestorm stops bad actors by making stolen data appear as unrecognizable puzzle pieces. The more data, the more unrecognizable puzzle pieces dispensed across different storage locations. See video.

Fragglestorm Features and Benefits

PLACE DATA SAFELY ANYWHERE

Data storage locations can be user assigned for meeting compliance, governance, and regulatory requirements.

TOTAL DATA PRIVACY

Companies are required to protect their customer and employee records. Fragglestorm makes unauthorized stolen data completely useless

STORAGE AGNOSTIC

Data is balanced across user allocated PC/laptop, on-premise storage devices, and multiple cloud service providers

For more information, please visit us at: www.cybervore.com

Fragglestorm's first feature product is called a Fragledrive© and uses an assignable letter drive. It protects data at its origin from the user out to cloud services. It operates transparently and requires no application changes. Each Fragledrive can assign on-premise storage devices and up to 64 cloud services to meet compliance, privacy, and regulatory requirements. Data access can be turned on and off via user command, smart device, and Bluetooth adding to a business's Zero-Trust data strategy.

Fragglestorm offers ultra-strong data protection that combines NIST's **A**dvanced **E**ncryption **S**tandard* and our fragmentation process creating unrecognizable encrypted fragments networkable anywhere. Only an authorized user can access their data using two or multi-factor authentication Identity Access/Management Services and FIDO devices to retrieve, reassemble, and decrypt their data.

* In July 2022, the NIST announced its quantum-resistant cryptographic algorithms. Cybervore will utilize these algorithms with Fragglestorm. The Advanced Encryption Standard (AES) Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce under Section 5131 of the Information Technology Management Reform Act of 1996.

System Requirements

- Licensed Software for Windows Laptops and Personal Computers, and Apple Computers
    - Single or multi-user seat licenses available – Ideal for hybrid work-from-home/office small to medium-sized businesses or individuals
    - Includes Fragglestorm's data security and privacy fragmentation process and Fragledrive's assignable letter-drive storage
    - Incorporates authentication services provided by Okta/Auth0
    - Uses the NIST advanced encryption standard (AES)-256-bit encryption combined with fragmentation. Cybervore does not develop its own encryption algorithms.
    - Included 24-hour by 7-day support and software maintenance updates
- Operating System Supported Versions and CPU/Memory Requirements
    - Microsoft Windows 8, Windows 10, and Windows 11 (All supported versions)
    - Intel processor at 2 GHz and faster (or compatible equivalent)
    - 1 GB of available RAM
    - Graphical Processing Unit (GPU) recommended
    - Runs on Apple macOS computers utilizing either Parallels or VMware Fusion.
- Hard Drive Space Requirements
    - 1 GB is required for installation
- Storage Devices and Services Supported
    - PC/Laptop storage drives
    - Network and Attached Storage devices or NAS
    - Removable hard drives
    - USB storage devices or thumb drives
    - Multiple hybrid cloud services; i.e.- Google, Box, Dropbox, and Wasabi Hot Storage services plus up to 60 others including S3 and immutable-compatible storage
    - Software-defined storage products or services are supported via the Fragledrive
- LINUX SUPPORT is planned for future Fragglestorm server and native cloud services.

Cybervore™