CYBERVORE

FRAGGLEdrive™

The disappearing, disk drive that renders your data useless to hackers

Available now: a hardened, certified, commercially supported single-user endpoint drive. FRAGGLEdrive™ is built on Cybervore's patented FRAGGLEstorm™ technology. It installs as a familiar software-only disk drive on a Windows PC or laptop and requires no additional hardware or changes to the file structure.

FRAGGLEdrive works seamlessly in the background to protect files the moment they are created. Data written to the FRAGGLEdrive is instantly encrypted and fragmented into unrecognizable "puzzle pieces," which are then unevenly distributed across one or multiple storage locations you choose. Only an authorized user can activate the FRAGGLEdrive and reassemble the data. When the drive is turned off, it disappears entirely, removing all access to the data and leaving no metadata or trail to follow.

Because protection starts at the endpoint where data originates and is stored, the FRAGGLEdrive extends a Zero Trust, defense-in-depth strategy beyond traditional perimeter and encryption-only approaches, rendering stolen or breached data useless to attackers.

HOW IT WORKS

- The FRAGGLEdrive installs as a standard disk drive on your PC or laptop (software only, no additional hardware).
- Protection begins at your device, where your data originates.
- Data is instantly encrypted and fragmented into unrecognizable puzzle pieces.
- Fragments are unevenly allocated across one or more user-assigned storage locations (on-premise, cloud, or a hybrid combination).
- Visibility of the FRAGGLEdrive can be toggled on or off through an identity access management (IAM) service such as Okta or Auth0.
- Only an authorized user can turn the drive on to access their data; turning it off removes all data accessibility.

KEY BENEFITS

Customizable Storage Tailor your virtual storage to fit your business needs.	**Enhanced Security** Extends your Zero Trust defense-in-depth strategy.
Seamless Integration No disruptions to your routine or applications.	**Strict Access Control** Only authorized users can access your data.
Flexible Data Security Choose where and how your data is stored to meet compliance requirements.	**Multi-Factor Authentication** Use MFA for easy, secure control of FRAGGLEdrive access.

TECHNICAL SPECIFICATIONS

Deployment	Software-only virtual disk drive — no additional hardware required
Operating Systems	Microsoft Windows 11 (PC/laptop); macOS support planned
Encryption	NIST Advanced Encryption Standard (AES) 256-bit encryption (optional)
Core Technology	FRAGGLEstorm™ patented Smart Data Fragmentation™, enterprise level protection
Identity & Access Management (IAM)	Single-user sign-on with personalized IAM services (e.g., Okta, Auth0)
Authentication	Multi-Factor Authentication (MFA) support
Storage Options	On-premise devices, cloud storage services, or hybrid / multi-cloud storage — user-assignable and allocated
Cloud Compatibility	Supports up to 70 consumer and commercial S3-compatible cloud services and on-premises networked and storage devices
Multi-Drive Support	Multiple FRAGGLEdrives are supported per PC or laptop, per license.
Setup	Built-in installer wizard for easy, IT-free user setup
Deactivation	Manual or automatic deactivation instantly removes all data accessibility
Support	Online and priority support, with direct access via email

SECURITY & COMPLIANCE

- Verified independently via third-party Security Penetration Testing, Functional Testing, and Static Code Analysis.
- Gives organizations full control over where protected data is stored, helping meet compliance requirements.
- Designed to resist both developing quantum decryption methods and traditional brute-force attacks.
- Mitigates double-pronged ransomware and extortion attacks by preventing attackers from reassembling exfiltrated data.

WHY FRAGGLEdrive

Unlike traditional storage or encryption-only solutions, Cybervore does not sell data storage. FRAGGLEdrive works with the infrastructure you already have, whether that's local drives, network-attached storage, or services such as Microsoft OneDrive, Box, Dropbox, Google Drive, or S3-compatible storage like AWS or Wasabi. The result is a cost-effective, user-friendly layer of protection that integrates without disrupting existing applications or workflows.

CYBERVORE, Inc. • info@cybervore.com • www.cybervore.com

FRAGGLEdrive™ and FRAGGLEstorm™ are trademarks of Cybervore, Inc. © 2026 Cybervore, Inc. All Rights Reserved.