Beyond Encryption: A New Way to Protect Your Most Sensitive Data

/ Cloud, Cyber Security, Data Protection



We all want a world where your most sensitive data becomes a digital ghost—invisible, untouchable, and utterly useless to anyone who tries to steal it. Enter Fragglestorm, a solution that's changing the game in data protection.

The New Face of Cyber Threats

Cybercriminals aren't playing by the old rules anymore. Today's attackers don't just want to lock you out—they want to hold your data hostage. Not only are your systems encrypted by ransomware, but they steal your data. Imagine the heart-stopping moment when you realize your most confidential information is now a commodity, auctioned to the highest bidder on the dark web's ruthless marketplace. One breach, one moment of vulnerability, and everything you've built can unravel in the silent, merciless click of a mouse.

Navigating the Cybersecurity Minefield: Small Business, Big Vulnerabilities

As leaders of small and medium-sized enterprises (SMBs and SMEs) you face unique hurdles in this challenging environment. Unlike your larger counterparts, you often grapple with significant resource constraints —a lack of dedicated cybersecurity professionals on staff and smaller budgets allocated to cybersecurity measures. Furthermore, cybersecurity awareness among your employees is often lower due to less frequent or comprehensive training.

Adding to these immediate concerns are looming future threats. The rapid advancement of quantum computing poses a significant risk to your current encryption. Quantum computers could potentially break the encryption algorithms that underpin much of today's data protection, putting vast amounts of your data at risk. This has given rise to "harvest now, decrypt later" attacks, where malicious actors collect encrypted data with the expectation of decrypting it once quantum computing capabilities become more widespread.

Fragmentation: The Ultimate Defense Strategy

Cybervore's Fragglestorm goes beyond traditional encryption by employing patented fragmentation technology. This process first encrypts your data (currently using 256-bit AES) and then divides it into multiple randomly-sized fragments. These fragments are unevenly and randomly allocated across one or multiple user-designated storage locations, which can include any combination of local storage, on-premises devices, and multiple cloud services.

Fragglestorm fragments are individually meaningless. To gain access to the contents of a file, all fragments must be collected, reassembled—in the correct order—and then decrypted. This multi-layered security ensures that even if a data breach occurs, the original data remains inaccessible, unrecognizable, and unusable to unauthorized users.

Fraggledrive: Simplifying Data Security

Cybervore is focused on effective, simple, and usable data security. Thus, Fragglestorm includes the Fraggledrive, a virtual disk in the vein of Microsoft OneDrive, Box, or Dropbox, with the assurance that all files in Fraggledrive are secure. This design makes Fragglestorm remarkably user-friendly, integrating seamlessly with existing applications and requiring no complicated IT setup. Users can easily download the software and begin protecting their data without disrupting their current routines.

A significant differentiator is that Cybervore does not sell data storage services. Instead, Fraggledrive leverages your existing storage infrastructure, whether it's local hard drives, network-attached storage (NAS) devices, or cloud services such as Microsoft OneDrive, Box, Dropbox, or Google Drive. This eliminates the additional cost and complexity of procuring and managing new storage solutions.

Fragglestorm offers a range of features and benefits that directly address your data security challenges:

Enhanced Security: The combination of AES 256-bit encryption and fragmentation creates a formidable defense, making breached and stolen data unreadable and unusable. This also provides robust protection against future quantum threats, ensuring data security in the long term.
Strict Access Control: Fragglestorm utilizes built-in identity access and management (IAM) services like Okta/Auth0 to ensure that only authorized users can turn on Fraggledrive and access their protected data. Multi-factor authentication (MFA) increases security by strengthening authentication.
Ransomware Protection: By fragmenting and distributing data, Fragglestorm prevents ransomware attackers from piecing together usable information, effectively mitigating the impact of double-pronged ransomware/extortion attacks that include data exfiltration.
Ease of Use: Cybervore designed the software to be user-friendly and transparent, with a simple setup process and seamless integration with existing applications. Users can install a basic setup without IT support.
Compliance and Risk Reduction: Fragglestorm allows users to control where their protected data is stored, enabling them to meet various compliance standards and reduce the risk of penalties.
Flexible Storage Options: Users have the flexibility to choose from on-premises, multiple cloud services, or a combination for storing their fragmented data. Fraggledrive supports up to 64 storage locations.
Easy Deactivation: Users can manually or automatically deactivate the Fraggledrive, instantly removing all data accessibility, further enhancing security when data is not in use.

Why This Matters

The cybersecurity landscape is fraught with danger, and the evolving tactics of cybercriminals, particularly in ransomware attacks, demand a more robust and innovative approach to data protection. SMBs and SMEs, often operating with limited resources and expertise, are particularly vulnerable. The impending threat of quantum decryption further underscores the limitations of traditional encryption methods.

Cybervore's Fragglestorm offers a compelling solution to these multifaceted challenges. By combining strong encryption with a unique fragmentation technology and leveraging existing storage infrastructure, Fragglestorm provides a cost-effective, user-friendly, and future-proof way to secure sensitive data. Its design ensures that even in the event of a breach, data remains unusable, mitigating the risks of extortion and non-compliance. If you're to fortify your defenses against modern cyber threats and ensure the long-term security and privacy of your data, Cybervore's Fragglestorm is a solution worth investigating.

Always-On Retail Becomes a Platform Requirement at NRF 2026

January 14, 2026

No Comments

At NRF 2026, HPE advances always-on retail with AI-native networking, edge insight, and fault-tolerant compute.

READ MORE

Agentic Commerce Moves From Concept to Control Plane at NRF 2026

January 14, 2026

No Comments

At NRF 2026, Google Cloud positions agentic commerce as a control plane with CX agents,…

READ MORE

StorMagic Expands EMEA Reach Through QBS Distribution Agreement

January 14, 2026

No Comments

StorMagic expands EMEA distribution with QBS, extending access to its edge virtualization and HCI portfolio…

READ MORE

Dynatrace Extends Observability Into Feature Control With DevCycle

January 14, 2026

No Comments

Dynatrace acquires DevCycle to unify feature flags, progressive delivery, and observability for cloud- and AI-native…

Orchestrating Intelligence and the Rise of AI-Native Application Development

January 12, 2026

No Comments

Explore how agentic AI, platform engineering, and observability are reshaping

Percona Spins Out OpenEverest to Put Open Governance at the Center of Data Ops

January 12, 2026

No Comments

Percona transitions Everest into OpenEverest, an independent open source

READ MORE

application development. Key insights and…

READ MORE

project focused on open governance for…

READ MORE

Author



Jack Poller

Principal Analyst Jack Poller uses his 30+ years of industry experience across a broad range of security, systems, storage, networking, and cloud-based solutions to help marketing and management leaders develop winning strategies in highly competitive markets.

Prior to founding Paradigm Technica, Jack worked as an analyst at Enterprise Strategy Group covering identity security, identity and access management, and data security. Previously, Jack led marketing for pre-revenue and early-stage storage, networking, and SaaS startups.

Jack was recognized in the ARchitect Power 100 ranking of analysts with the most sustained buzz in the industry, and has appeared in CSO, Althority, Dark Reading, SC, Data Breach Today, TechRegister, and HelpNet Security, among others.