FENIXPYRE

THE SECURITY LAYER

FOR CLOUD FILE HOSTING, SHARING, AND COLLABORATION

SECURITY OF CLOUD-STORED FILES

Cloud data hosting and management solutions (e.g., OneDrive, Sharepoint, Box, Dropbox, Google, Egnyte, etc.) are built to provide a secure, scalable, and collaborative platform for storing, version controlling, sharing, and managing digital files. Moving storage to the cloud enhances productivity, improves data security, and supports compliance requirements, making it a valuable asset for both individuals and organizations.

For many organizations, cloud file hosting augments the existing traditional IT infrastructure, which has been predominantly on-premises. The value of cloud storage is in the way it seamlessly extends the collaboration options, without changing the way employees access, share, and work together on files. Typical users have a business account on the main provider the company has subscribed to, as well as others at the same time. Files are continually syncing with their personal desktop drives, possibly mapped to local file servers. As a result, organizations find it increasingly difficult to keep the business-related files in a single hosting solution. They get diffused beyond control, as users freely access and share these files with other solutions and mechanisms.

Flow of data across different locations is the leading cause for the notorious insider problem. Organizations lose control of their data as the employees and partners start collaborating over other personal cloud solutions as well as classical media such as email and removable drives. Organizations try to address this issue via Data Loss Prevention (DLP) solutions (e.g., Microsoft Purview), which have their own problems, including but not limited to management complexity and poor user. experience (1; 2).

Toward that end, FenixPyre offers a major value add to business cloud file hosting and management solutions. FenixPyre eliminates the data flow control problem and unifies the collaboration options across the hybrid IT ecosystem with added complete security. It acts as the security layer encompassing the entire set of file stores, including cloud, file server, and desktop. FenixPyre offers a significantly enhanced capability set without sacrificing the usability and simplicity of cloud storage solutions.

DESKTOP SYNC

Files maintained over a cloud store get synced over a desktop through an agent deployed. Typical business users maintain multiple cloud hosting solutions, sync'ing simultaneously over their personal computers, as illustrated in **Figure 1.** Further, organizational data can be maintained over multiple stores, including the file servers, virtual machines, etc. Businesses would like to control the flow of files to eliminate the loss of business data through insider actions. Solutions like Box, Google, OneDrive have built-in capabilities to keep the files in house, as long as the file is kept solely on the cloud store. However, once synced to the desktop, files start moving freely. Users can push them to other cloud stores or removable drives. They can be accessed by all applications, including personal email, messaging applications, etc.

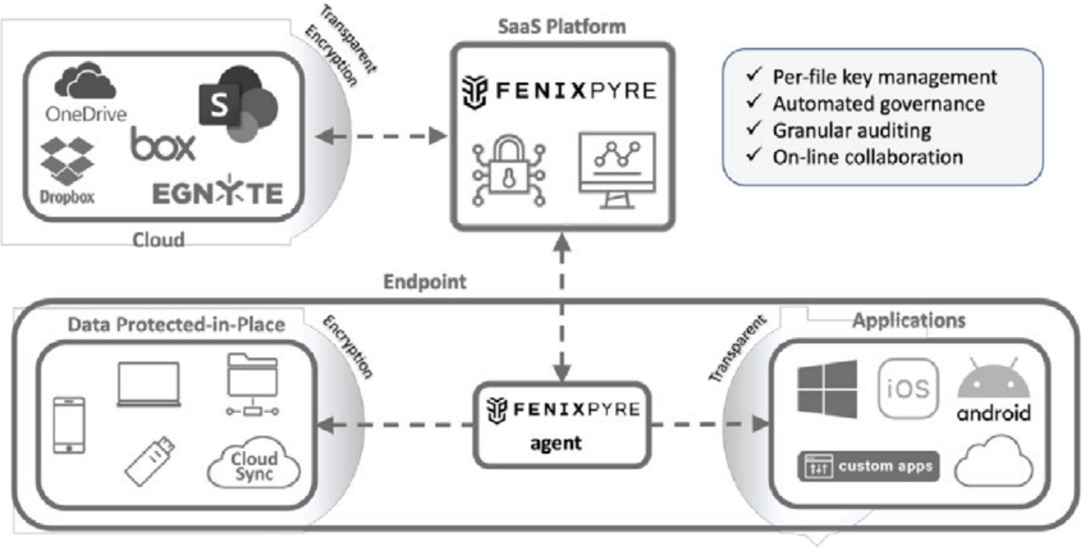


Figure 1: FenixPyre integrated into the enterprise IT ecosystem

FENIXPYRE SYNC [FPO TITLE]

FenixPyre anchors the files to the desired cloud store even on desktop and as a result eliminates the flow of data out of the organization by insiders, departing employees, or ransomware attackers. FenixPyre can be set up such that, the only way to access a file will be directly in the folders specified by the organization. It would not eliminate the possibility of external on-line collaboration, as it is provided by FenixPyre with full control retained by the organization. For example, for collaboration over Microsoft Office files, FenixPyre provides co-editing capability over on-line O365 with proper access controls including restricted access, link expiry, password-protection, and other attribute-based access controls as desired by the organization.

In **Figure 2**, we illustrate the data flow architecture for FenixPyre's cloud store integration with extension to the sync agents on the desktop. Each sync agent for a cloud store is deployed on a custom file system built on the minifilters and driver modules provided by the operating system. Similarly, FenixPyre's agent is built on its own file system that uses Windows-native minifilters. FenixPyre's kernel mode components are adjusted to align with the file system managers of the cloud sync agents to be able to proactively encrypt and protect files before they are transferred to the local store. As a result, no plaintext version of a file will be synced up outside of the device to the cloud. All versions edited on the desktop applications will remain encrypted on the cloud at all times.

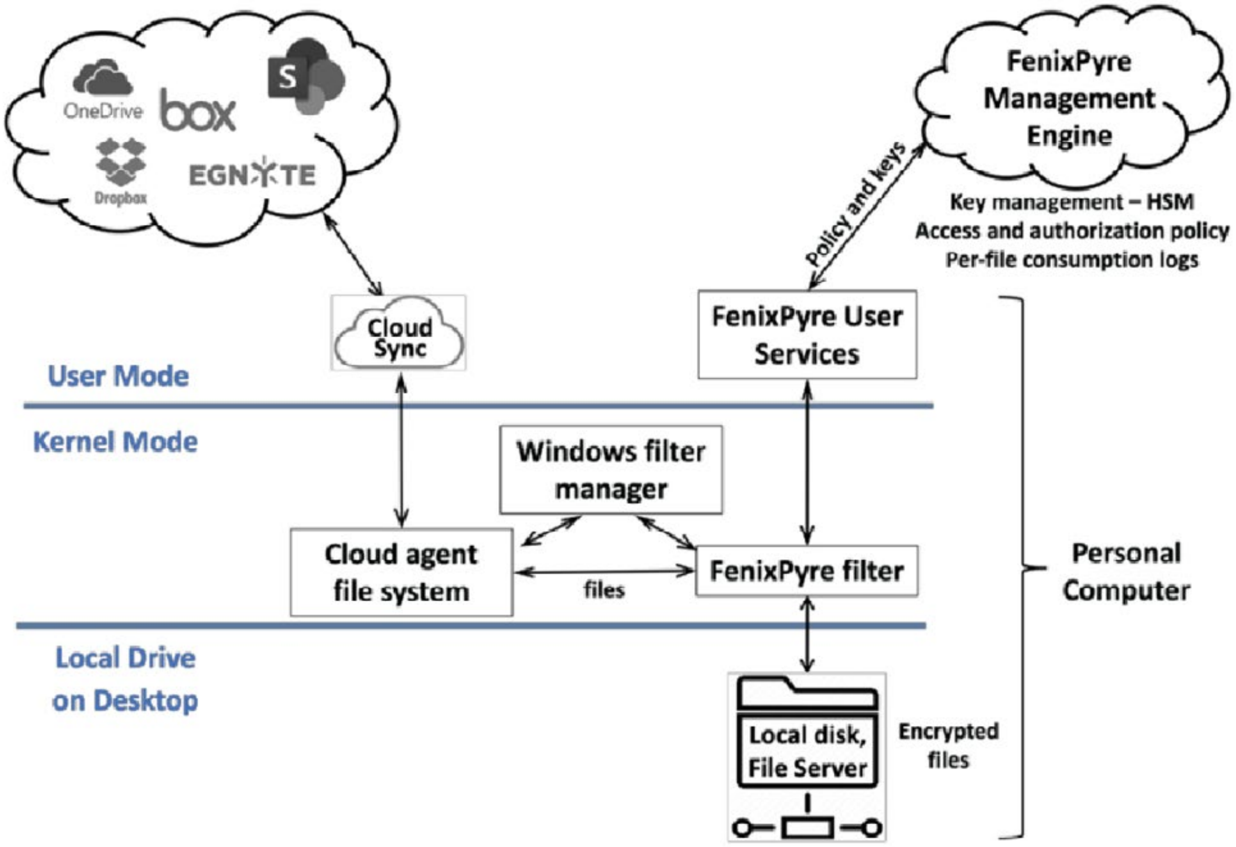


Figure 2 The local cloud agent and FenixPyre are built on a separate file system, managed by the filter manager. Interoperability may require a change in the filter source codes.

MULTI-CLOUD AND HYBRID STORAGE SUPPORT

As mentioned, a typical organization is hybrid with users having multiple cloud data management solutions as well as file servers set up simultaneously. Traditionally, operation and security of these different components need to be handled separately and independently. The cloud file hosting solution the company subscribed to can only manage its own store.

FenixPyre addresses this issue with a **unified rules and policy engine** that works on-premises and across multi-cloud environments to make secured file sharing and collaboration seamless and easy to promote continued productivity. Management, activity monitoring, and rules enforcement are all maintained over a **single administrative dashboard**, designed to simplify the data governance and security management effectively across the entire ecosystem.

ZERO-TRUST AND ZERO-KNOWLEDGE

When an organization subscribes for a cloud hosting provider, they give them the ability to not only host the files and manage versions, but also the ability to access the content of the files hosted, since the provider controls the encryption keys. This creates a clear violation of **the least privilege principle** and leads to a single point of failure for data losses. For example, if a user loses his/her login credentials, all files can be exfiltrated easily. Further, private customer content can be utilized by the cloud provider to improve their product line (e.g., training AI).

To alleviate these concerns, FenixPyre bakes **zero-trust down to each file** individually via strong encryption. Due to its added transparent encryption, FenixPyre proves zero-knowledge with respect to the cloud provider hosting the data without adding any degradation on the functionality of the hosting solution (i.e., hosting, version control, access control, etc.). Further, with the ability of the master key to be controlled by the customer, even FenixPyre the company, can be kept oblivious to the content. **With FenixPyre, the customer has full control of their own content.**

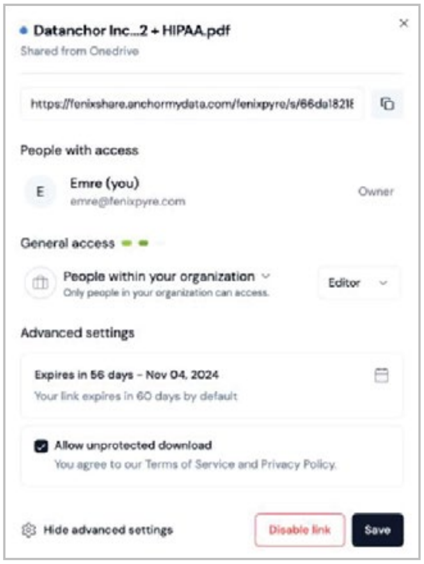
Note that, some DLP solutions such as Purview also offer Double Key Encryption (DKE) integration via their platform, but the plain DKE brings an extremely limited user experience, since it eliminates the possibility of using on-line editing via O365 or even sharing and collaboration of files. With Purview, the desktop remains the only way to access such files. FenixPyre inverts this equation by adding the DKE capability to Purview without eliminating the on-line (web) editing as well as collaboration with external users. **FenixPyre enables all the benefits of the native O365 experience with security and full control of the content retained by the customer.**

SHARING AND COLLABORATION

FenixPyre provides a universal sharing and collaboration experience across the cloud store platforms. The architecture of the platform is illustrated in **Figure 5**. Any access architecture is serverless, and the service request initiates the creation of a temporary service on which edit operations are executed via O365 editors. Even during the editing of the file on FenixPyre, the source file remains encrypted on the cloud store. The changes made are automatically written back on the store as a new version, after they get encrypted; as a result there remains no plaintext version.

Fenixpyre has direct integration at the UI level on the cloud and the users can access the FenixPyre menu, enabling file/folder sharing, access, encryption/decryption of the files, as well as access logs as shown in **Figure 3**. Access and co-edit experience is on FenixPyre, universal across all users including the home user and the remote collaborator.

The sharing dialog box, in **Figure 4**, gives the ability to the users to add/remove collaborators, make access rules and deadlines to the document for remote users, which receive the access link automatically from the FenixPyre sharing platform. The home users can manage all of their access links and rules from a unified FenixPyre Sharing Management Console, shown in **Figure 6.**



Datanchor Inc...2 + HIPAA.pdf
Shared from Onedrive

https://fenixshare.anchormydata.com/fenixpyre/s/66da1821E

People with access

E Emre (you) emre@fenixpyre.com Owner

General access

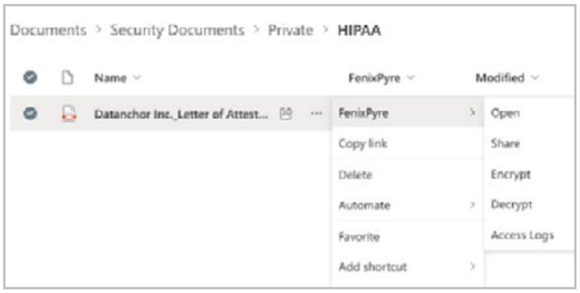
People within your organization
Only people in your organization can access.
Editor

Advanced settings

Expires in 56 days – Nov 04, 2024
Your link expires in 60 days by default

☑ Allow unprotected download
You agree to our Terms of Service and Privacy Policy.

Figure 3



Documents > Security Documents > Private > HIPAA

Name | FenixPyre | Modified

Datanchor Inc._Letter of Attest...

Figure 4

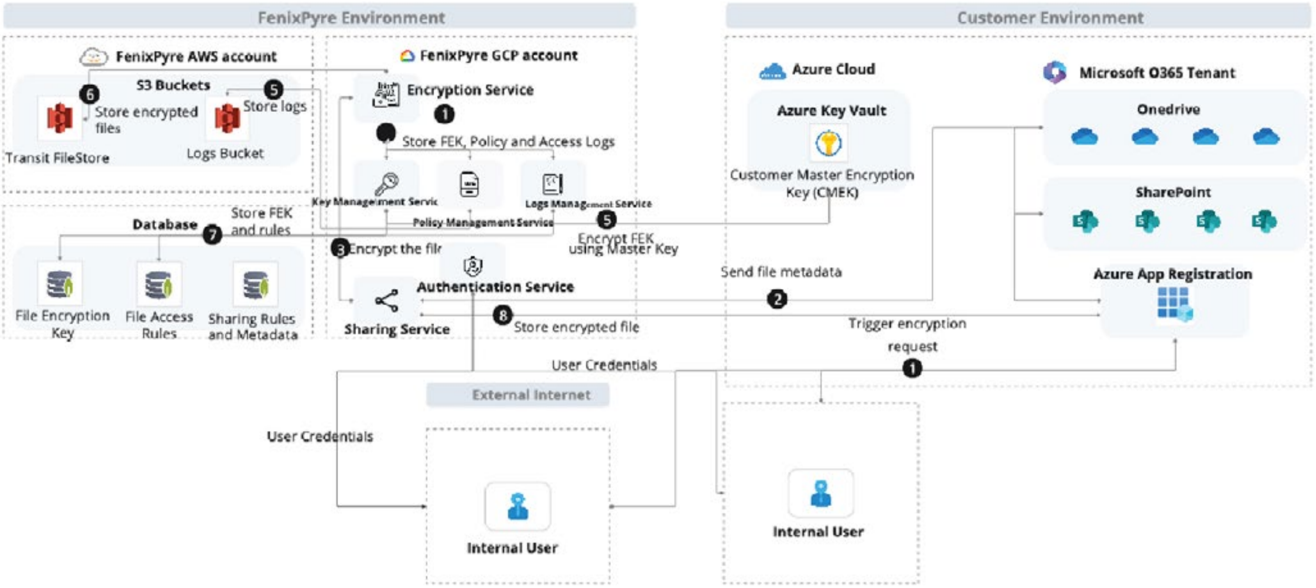
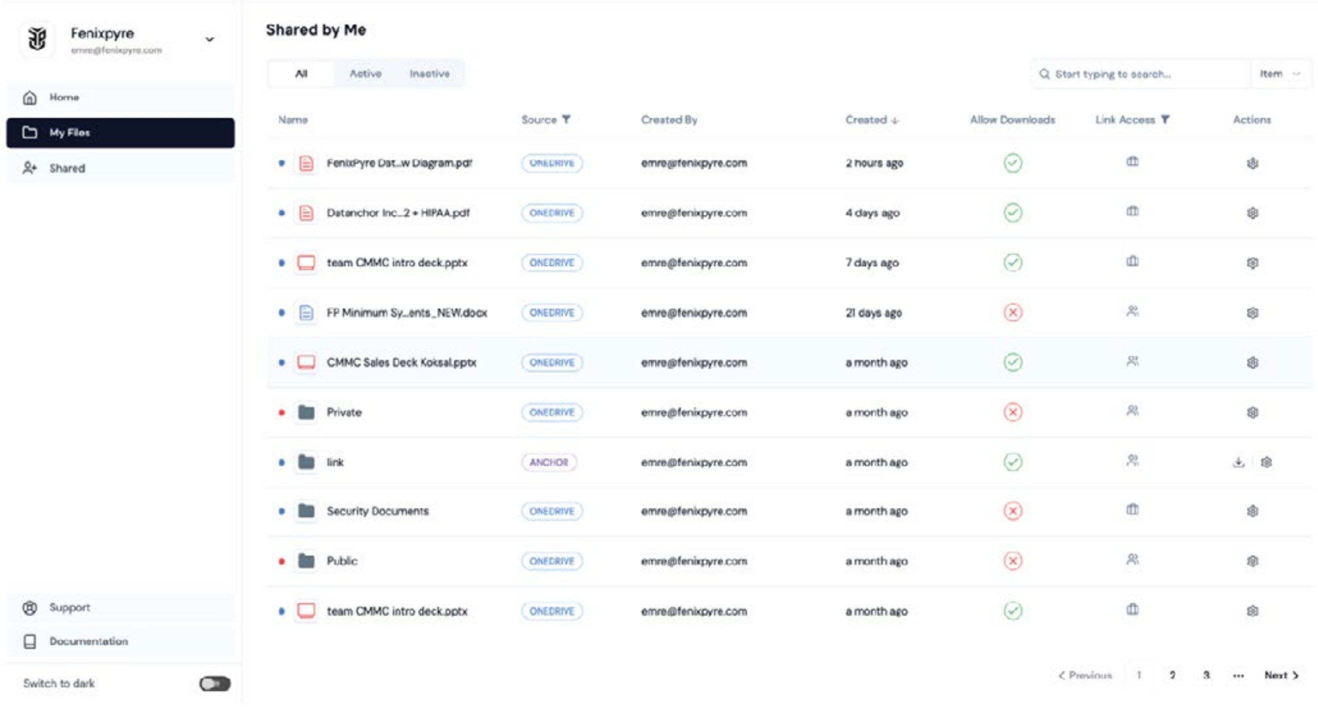


Figure 5: The universal sharing and collaboration architecture of FenixPyre. Files remain encrypted at the store at all times, even when they are actively being co-edited on the FenixPyre sharing platform.



Shared by Me

Name	Source	Created By	Created	Allow Downloads	Link Access	Actions
FenixPyre Dat...w Diagram.pdf	ONEDRIVE	emre@fenixpyre.com	2 hours ago	✓		
Datanchor Inc...2 • HIPAA.pdf	ONEDRIVE	emre@fenixpyre.com	4 days ago	✓		
team CMMC intro deck.pptx	ONEDRIVE	emre@fenixpyre.com	7 days ago	✓		
FP Minimum Sy...ents_NEW.docx	ONEDRIVE	emre@fenixpyre.com	21 days ago	✗		
CMMC Sales Deck Koksal.pptx	ONEDRIVE	emre@fenixpyre.com	a month ago	✓		
Private	ONEDRIVE	emre@fenixpyre.com	a month ago	✗		
link	ANCHOR	emre@fenixpyre.com	a month ago	✓		
Security Documents	ONEDRIVE	emre@fenixpyre.com	a month ago	✗		
Public	ONEDRIVE	emre@fenixpyre.com	a month ago	✗		
team CMMC intro deck.pptx	ONEDRIVE	emre@fenixpyre.com	a month ago	✓		

Figure 6: FenixPyre Sharing Management Console

SECURE FILE SHARING AND COLLABORATION MADE EASY

Files are the new perimeter for global businesses – keep them safe anytime, anywhere – at rest, in transit, in use, while sharing and collaborating. FenixPyre is the simple answer to a complex problem.

FenixPyre simplifies secure cloud file sharing by protecting data at the file level, ensuring that sensitive information remains secure whether at rest, in transit, or in use. Built on a zero-trust model, FenixPyre integrates effortlessly into your existing workflows without disrupting productivity or requiring major IT investments.

1. FenixPyre Technical Reports. FenixPyre as a Value add to Purview. [Online] 2024. https://share.anchormydata.com/fenixpyre/s/666a91117aba3e89e941166a/fenixpyre%2520on%2520purivew.pdf.

2. FenixPyre Technical Reports. FenixPyre Positioning and Strategy Analysis for the DLP Market. [Online] 2024. https://share.anchormydata.com/fenixpyre/s/666a91da7aba3e3aab41166d/fenixpyre%2520dlp%2520positioning%2520and%2520strategy.pdf.

FENIXPYRE