FENIXPYRE

# DATA-CENTRIC SECURITY ARCHITECTURE

## ZERO-TRUST BAKED DOWN TO THE DATA LAYER

# ABSTRACT

**Traditional Data Loss Prevention approaches have failed to eliminate data losses. From an IT perspective, the DLP solutions have complicated controls and management, and from a user perspective they have a highly frustrating user experience.**

FenixPyre inverts the equation with a unified rules and policy engine that works on-premises and across multi-cloud environments to make data theft irrelevant by applying zero trust to the files themselves. FenixPyre's data security is differentiated by its ability to keep files encrypted both in use and accessed outside the organization in collaboration mode. **As a result, files remain protected even if they are stolen.**

FenixPyre remains invisible to the business users (like antivirus) so that files are free to travel and security doesn't impact productivity or workflows. FenixPyre can be deployed within a few hours and provides integrations to modern Identity and Access Management (IAM) and Security Information and Event Management (SIEM) Platforms. Management is straightforward and provides visibility via its file-level forensic logging and access revocation even after a loss, making data theft irrelevant.

## WHAT IS A SECURITY ARCHITECTURE?

A Security Architecture is the technical design of your information system, including what is in it, how it all fits together, and how it enables controls to implement the level of security to keep your data protected. In this document, we provide some of the specifics of the security architecture FenixPyre provides as the files are stored locally on prem or in a cloud store. **The focus for this paper is the protection for local access; security for sharing and collaboration is covered in another whitepaper, made available upon request.**

### SECURITY ARCHITECTURE

In this section, we provide the proposed security architecture with the FenixPyre platform. The architecture is simple and broad; it applies to a variety of business scenarios, covering a wide range of industries with different IT infrastructures - from very elementary to sophisticated and hybrid.

The proposed architecture is illustrated in Figure 1. With FenixPyre, the "system" is the set of FenixPyre-enabled devices containing sensitive files. FenixPyre simplifies compliance and data security by reducing the system boundary from a complex network to a narrow set of encrypted files that are end-to-end encrypted by Microsoft CNG modules with FIPS-validated cryptography [CMVP].

## THE HIGH-LEVEL ARCHITECTURE

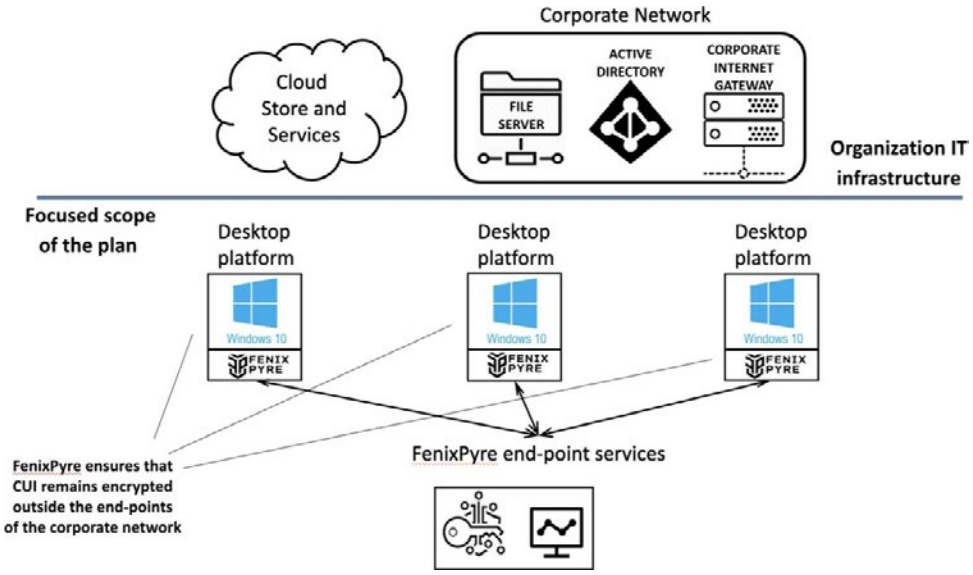


Figure 1: FenixPyre simplifies CMMC compliance by reducing the system boundary to a narrow set of encrypted files that are accessed and processed at the FenixPyre-enrolled endpoints (below the blue line). CUI is end-to-end encrypted by FenixPyre with FIPS-validated cryptography. The compliant architecture is independent of the IT infrastructure (above the blue line). Thus, the mapped domains are covered for a broad set of organizations with various sophistication.

At the heart of the FenixPyre architecture lies the fact that encrypted sensitive files can only be consumed at FenixPyre-enabled endpoints due to the robust end-to-end encryption system integrated into the desktop platform built by FenixPyre. The key management and audit logging services are both provided by the FenixPyre platform, external to the desktop agent. These services provide the secure access management and audit log creation in coordination with the desktop platform, with components orthogonal to the rest of the organization's IT infrastructure (above the blue line in Figure 1), making the implementation of the security plan **simpler, lower cost, and more robust.**

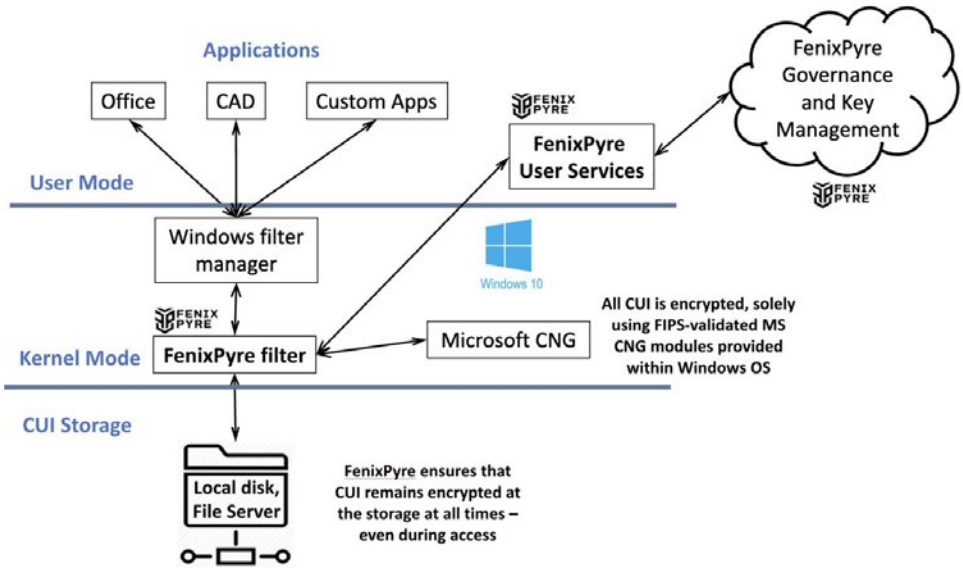


Figure 2: CUI is accessed in plaintext only from endpoints. All CUI remains encrypted at the storage at all times, even during access by applications or while sharing and collaborating. Encryption is only done by FIPS-validated Microsoft CNG Modules. FenixPyre operates in FIPS-mode and it merely conducts the data flow between the store and the applications to enforce CMMC controls. No module outside of MS CNG deals with encryption or decryption of CUI.

End-point users are managed by Active Directory (local or Azure). The sensitive files can be stored on a network drive or a local store, but they cannot be decrypted on those drives due to end-to-end encryption. As the protected files are always encrypted at rest, each device containing such files is treated as a mobile device. The end-point architecture is illustrated in Figure 2.

### FIPS COMPLIANCE

All encryption and decryption are done via FIPS-Validated Microsoft CNG modules and FenixPyre conducts the flow of data in accordance to the CMMC controls. The Microsoft CNG Modules provide encryption via the Federal Information Processing Standard (FIPS) 140-2 mode. FIPS 140 is a cryptographic security standard used by the federal government and others requiring higher degrees of security in order to comply with NIST requirements for data protection.

**FenixPyre only utilizes the certified and unmodified encryption modules available within the Microsoft Operating Systems within desktop and server.** Consequently, FenixPyre will not show up in the NIST Cryptographic Module Validation Program vendor lists. When the FIPS mode is enabled via the registry, encryption in all FenixPyre filter workflows use FIPS-approved algorithms during the encryption and decryption of FenixPyre protected files passed back and forth between the applications and the storage. At the time of this writing, the active certificate is #4536 which has a sunset date of 09/21/2026. Details of the module can be accessed from the link provided above.

## EXAMPLES OF IT INFRASTRUCTURES

In this section, we provide a few IT architectures with relevant use cases. As discussed in the last section, end-to-end encryption provided over the FenixPyre platform supports the security architecture for internal collaboration over a variety of use cases (illustrated in Figure 3).

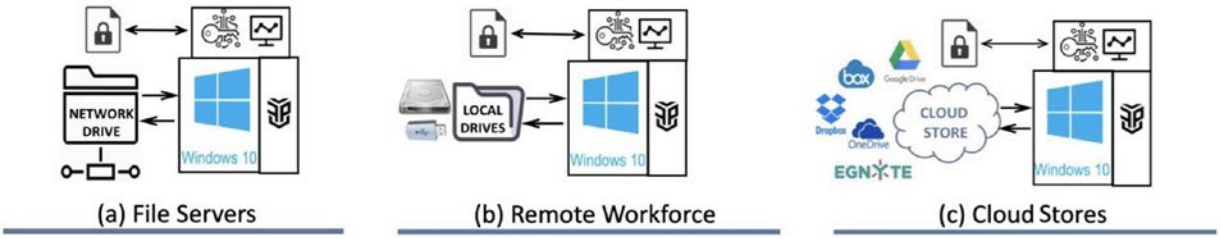


Figure 3: End-to-end encryption across endpoints makes it possible to collaborate on unstructured data over a variety of data stores.


Figure 4: FenixPyre platform has support for a wide variety of applications that encompass CAD and Office. It enables secure and no-friction access and collaboration on the associated files.

Many organizations keep CUI internally within their network at local file servers (mainly over Windows Server OS). For example, **manufacturing, construction**, and **high-tech engineering** organizations, building products and IP for the DoD use a variety of file types and applications, including CAD and Office. FenixPyre keeps the designs, associated IP, contracts, and calculations encrypted in the file server, while enabling access from the desired applications, a few of which are shown in Figure 4, **without a change in the workflow or the application itself.** Directories and CUI files are stored on a network drive but cannot be decrypted on that drive due to end-to-end encryption.

**As a result, CUI is protected automatically as per CMMC, while the organization does not lose any efficiency in processing the data.**

With the pandemic, organizations have a considerable amount of their workforce needing to access CUI remotely. In such cases, files are downloaded to the local drives for processing. This is sometimes despite the policies on VPN use, due to the performance issues associated with remote consumption. Such local store and access inflate the attack surface and makes the CUI policies difficult to enforce.

With the FenixPyre platform, this would not pose a problem. An admin can simply include the local drive as a protected area and make sure that the CUI remains safe, even when accessed remotely by the employees or contractors.

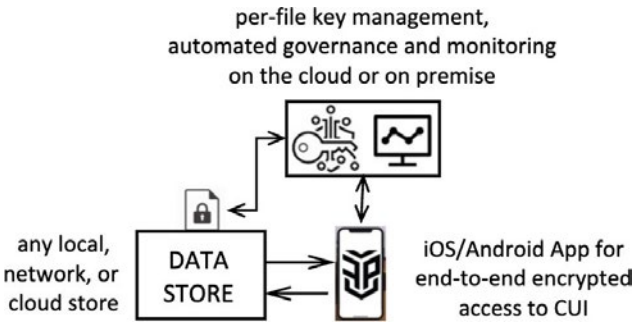


Figure 5: FenixPyre's protection extends to a Mobile App for iPhone and Android platforms. As a result, CUI can be accessed from smart phones and tablets.

- Organizations are moving to a hybrid IT infrastructure with cloud applications and data stores involved in everyday processes. Most organizations will have certain processes handled over FedRAMP High government clouds such as Microsoft GCC High. However, it is likely that there will be applications and processes involving CUI on commercial cloud as well. The FenixPyre platform provides the flexibility of protecting data on commercial cloud due to its robust end-to-end encryption integrated.
- **DFARS 7012** and **ITAR** have additional requirements, such as information must not be exported out of the United States. This creates an obstacle to using commercial cloud storage because commercial clouds store data outside the US and are administrated by people outside the US. However, they carve out an exception when the information end-to-end encrypted with FIPS-validated cryptography. With FenixPyre end-to-end encryption you can store data on commercial clouds and still be compliant.

## DATA FLOW DIAGRAM

For the FenixPyre security diagram given in the previous section, a detailed data flow diagram is provided in Figure 6. The diagram illustrates the data structures and types that are exchanged across the components of FenixPyre. All CUI access happens within the CUI access points, where the encryption and decryption of the CUI takes place. FenixPyre eliminates the possibility of any CUI content to be taken out of the access point. The only communication outside involves policy and key exchange, both of which are executed over an end-to-end encrypted (via Microsoft TLS modules) channel.

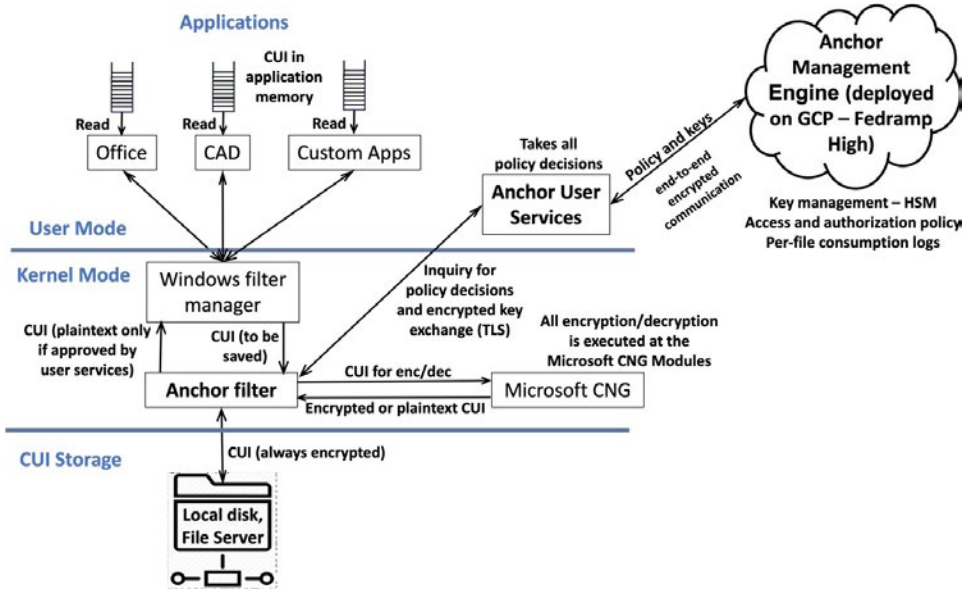


Figure 6: FenixPyre data flow diagram. This diagram details the data structures and types exchanged across different blocks within the security architecture.

## DATA PROTECTION WITH FENIXPYRE DATA-CENTRIC SECURITY

FenixPyre removes the complexities of data security management, ensuring continuous protection of sensitive data and collaboration without compromise. File-level encryption creates a self-protecting perimeter that follows the data – at rest, in transit, or in use. The FenixPyre platform embeds zero-trust, data-centric security into any file using a patented combination of military-grade FIPS-validated encryption and multifactor access controls. FenixPyre integrates effortlessly with existing workflows, eliminating user friction and easing compliance. Whether on-premises, in the cloud, or across multi-cloud environments, FenixPyre delivers comprehensive protection that helps meet regulatory mandates like CMMC, mitigates insider threats and ransomware, and supports data governance. OPTION 2: FenixPyre removes the complexities of data security management to continuously protect sensitive data across environments and facilitate collaboration without compromise. Focusing on data-centric security, FenixPyre shrinks compliance boundaries, enforces zero trust at the file and folder level, and employs non-persistent data to reduce the impact of security incidents like ransomware. Encryption at the file level creates a self-protecting perimeter that follows the data – at rest, in transit, or in use. Seamless integration with existing workflows eliminates IT and end-user friction and eases compliance. FenixPyre delivers comprehensive protection that helps meet regulatory mandates like CMMC, mitigates insider threats and ransomware, and supports data governance.