

The Components of the FileFlex Zero Trust Architecture

FileFlex Enterprise has a unique patented architecture designed to:

1. Protect confidentiality of sensitive information by providing access to data without providing access to the organization's network infrastructure
2. Provide IT the tools they need to control file sharing
3. Protect the transfer of information
4. Allow for only authorized access to content and,
5. Protect user credentials

The FileFlex Enterprise solution is comprised of 3 main components. All 3 components are required in order to make the solution work. The 3 components are:

- FileFlex Enterprise server (and PKI server)
- FileFlex Enterprise Connector Agent
- FileFlex Enterprise Client App

All 3 components use encryption (AES256 symmetric encryption) in various ways in order to protect the user data, internal data, tokens and communication channels. The use of encryption coupled with architectural design and process flow ensures privacy, security, protection of credentials and authorized access to content.

Diagram 1 outlines a high-level architecture of the overall solution and a logical view of the interaction between the broader 3 main components of the system.

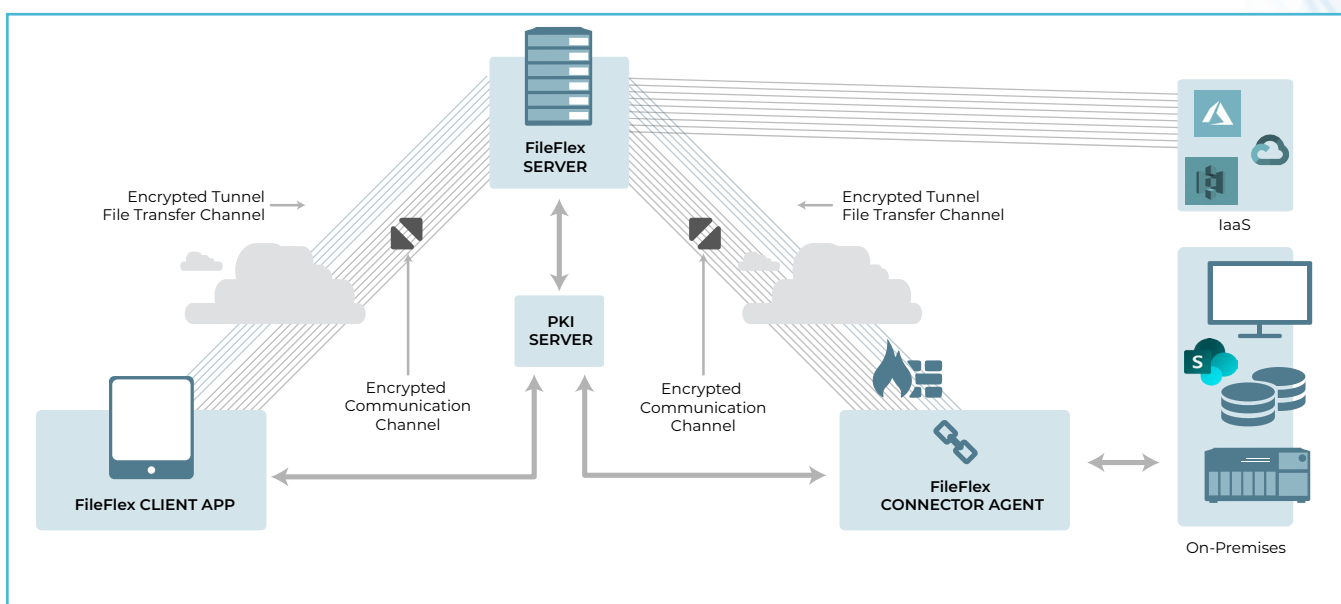


Diagram 1 - Zero Trust Architecture of FileFlex Enterprise

The FileFlex Enterprise Server

The FileFlex Enterprise Server is a public facing server that is accessible on the internet and provides access to the service. The server manages access rights to the service by validation and authentication and acts as a relay service between the authenticated users and the content sources that they have rights to access. The FileFlex Enterprise server does not hold any user content data and only manages and enforces the rights and permissions of authorized users of the system. It acts like a switchboard to connect users to their files in their source locations and like a policeman to enforce access policies. Thus, it helps protect the organization because it does not store any files or content and it does not store any credentials.

It is important to understand that the FileFlex Enterprise server is actually a cluster of servers that act together to behave as one and provide the functionality of the FileFlex server / service. It is also important to understand that all the server components mentioned here are virtual servers and not physical appliances and reside in a VM on a single physical machine. However, most of these individual server components may be spread across different physical machines in the cluster for enhanced robustness and security.

The public-facing FileFlex Enterprise 'web' servers are separated from the protected connector agents by a firewall. The public servers are responsible for communicating with the FileFlex users, while the connector agents are responsible for accessing remote data.

“The FileFlex Enterprise server does not hold any user content data and only manages and enforces the rights and permissions of authorized users of the system”

All external server communications are performed on encrypted channels. The FileFlex Enterprise server only communicates with the connector agent & client application. Connections are made using HTTPS. The server uses dedicated ports to communicate with both the FileFlex connector agents and the FileFlex client

application which must be open inbound to server and open as bidirectional.

FileFlex Enterprise PKI Server

“The FileFlex Enterprise PKI server offers double encryption, which is a feature that allows end-to-end encryption from source all the way to destination”

A public key infrastructure (PKI) is a set of roles, policies and procedures needed to create, manage, distribute, use, store & revoke digital certificates and manage public-key encryption.

The FileFlex Enterprise PKI server offers double encryption, which is a feature that allows end-to-end encryption from source all the way to destination. This is a very effective protection against man-in-the-middle and impersonation, snooping and intercept to provide very strong security of data transfers. When selected, the content owners will be able to select whether or not they want to enable double encryption on a per-content-source basis. A side effect of such a configuration (when double encryption is enabled by the content owner) is that the content cannot be consumed from a web browser. Users will still benefit from traditional single tunneling encryption as well as other security options, which allows for browser-based content consumption.

The FileFlex Enterprise Connector Agent

The FileFlex connector agent is a software only component that runs on a device located on the corporate infrastructure behind the corporate firewall. The connector agent can access any device or storage located on the same infrastructure, on behalf of the user using the local permissions of the user. The main purpose of the connector agent is to perform requested task (access, relay and manipulate data) located on the same infrastructure, on behalf of a user as if the user were physically present on that infrastructure. The connector agent is also responsible for encryption and decryption functions for all data transmission, as well

as managing revisioning and aspects of collaboration functions.

There exist multiple flavors of the connector agent for all types of devices, OS & architecture.

OS: Windows, Mac, Linux
CPU: Intel, ARM
Devices: NAS, Routers, Servers, Desktops, Laptops

“The connector agent is also responsible for encryption and decryption functions for all data transmission.”

All external communications from connector agent to the FileFlex Enterprise server are performed on encrypted channels. Connections are made using HTTPS. The connector agent is designed to only communicate with the FileFlex Enterprise server by establishing an outbound connection using a number of secure measures to ensure that connections are only to designated FileFlex servers. By establishing outbound connections, this ensures that no new ports need to be open on the corporate firewall thus eliminating the risk of external access to the connector agent inside the corporate infrastructure. The connector agent uses dedicated ports to communicate with the FileFlex server which must be opened outbound only and as bidirectional.

FileFlex Enterprise Client App

The FileFlex Enterprise client app provides a mechanism for the user to access, browse, manipulate and share any content from a single dashboard. The FileFlex Enterprise app works in conjunction with the FileFlex server to allow the user to perform these actions securely with assigned privileges and enforce permission activities such as download, view-only, edit and upload. FileFlex does not use link-based sharing. Every user must log into the system using the client application, be authenticated to the server, their privileges are communicated and bound to their app. The client app, in conjunction with the server, assists in enforcing the rules and privileges assigned to the

user. When FileFlex generated links are used and copied into an email, the link never gives direct access to the content. Instead FileFlex generated links open the FileFlex app and authenticate the user. This user authentication is a key component to give IT control and tracking over the file sharing of the organization and to mitigate against spoofed trusted sources.

FileFlex Enterprise is account-based, not device-based, meaning a user logs into their account from any device – whether Windows or Mac PC, or iOS or Android smartphone or tablet, or web browser. When the user logs in, they get access to every connector agent that is bound to their account as determined by IT and enforced by the server. Those agents can be located on any and every network and facility the organization has globally and all accessed through the client app via a single-pane-of-glass dashboard and bound to the users account to allow access, sharing and collaboration of any file in the organization no matter where located all the while staying under the control of IT.

“The connector agent is designed to only communicate with the FileFlex Enterprise server by establishing an outbound connection using a number of secure measures to ensure that connections are only to designated FileFlex servers”

All external communications are performed on encrypted channels. Connections are made using HTTPS. The client app is designed to only communicate with the FileFlex Enterprise server on outbound bidirectional communication channels. The client app uses dedicated ports to communicate with the FileFlex server which must be open as bidirectional.

How It Works

When a user wants to access, share, collaborate, stream or manage something, they navigate to and click the file in the client app. The client app makes a request to the FileFlex Enterprise server and the server determines whether the user has the privilege

to access and perform the request. If it does, the server knows the connector agent that the user is bound to that has the data. The server contacts the connector agent and forwards the request along with a unique token ID to the connector agent. The connector agent receives the request along with the token ID which it uses to pull the user's AD/LDAP credentials from its encrypted DB. The connector agent then impersonates the user and navigates the infrastructure and performs the request on behalf of the user using the user's credentials. The connector agent accesses the data, encrypts the data and streams it over the encrypted communications tunnel back to the user almost instantly.

“Every user must log into the system using the client application, be authenticated to the server, their privileges are communicated and bound to their app.”

“Seamlessly supports secure zero-trust access, sharing and collaboration from dedicated IaaS servers with suppliers such as Amazon, Azure and Google”