Zero Trust Remote Data Access and Collaboration - *Technology Architecture*

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.

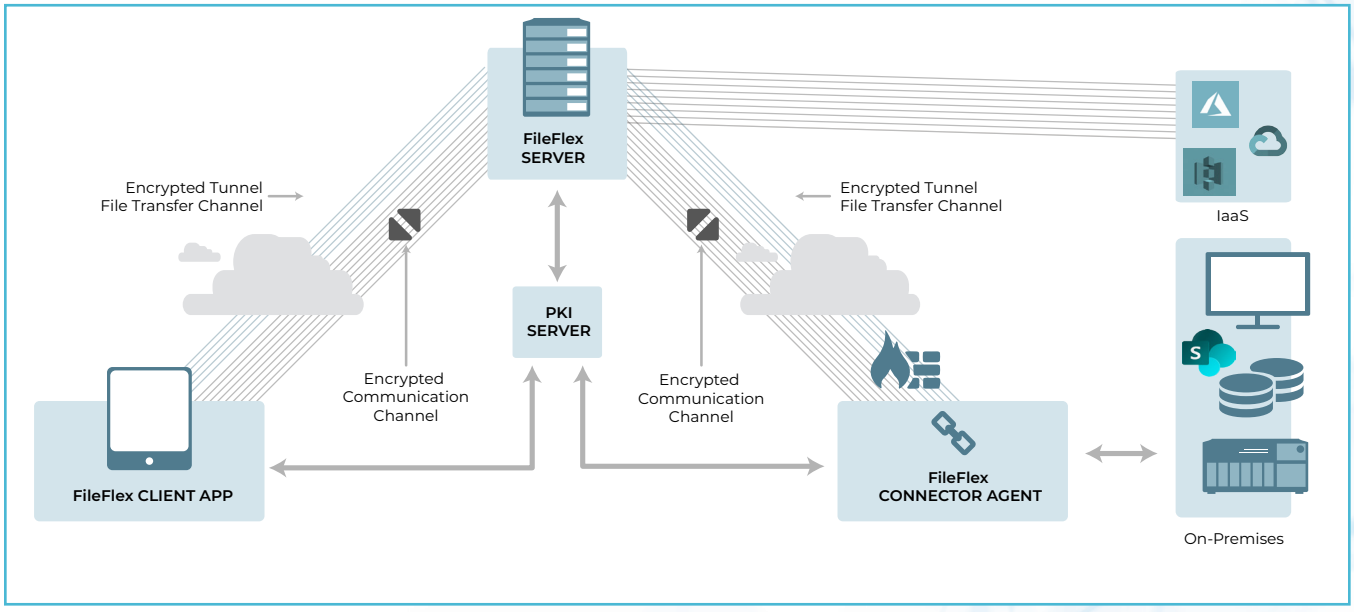

Diagram 1 - Zero Trust Architecture of FileFlex Enterprise

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 it's 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"

FileFlex Enterprise Hardware Requirements

Version 05052020

Server Hardware Requirements

The following table describes typical deployment configurations and capacities. Server hardware refers to VM-assigned resources.

	Minimum	Mid-Range	High-End
CPU	Intel Core i3 2-Core @ 2ghz Supports VT-x and AES-NI	Intel Core i7 4-Core or 6-Core @ 3ghz Supports VT-x and AES-NI	Intel Xeon 8-Core or 10-Core @ 3ghz Supports VT-x and AES-NI
RAM (assigned to VM)	4gb	8gb	16gb
Network	Single 1GbE LAN Port	Dual 1GbE LAN Ports w/ Aggregated Links	Dual 10GbE LAN Ports
OS	Linux based, with integrated virtualization support	Linux based, with integrated virtualization support	Linux based, with integrated virtualization support
Maximum Concurrent View-Only Conversions	1	3-4	6-8
Max Activations and/or Users	1000	2500	5000
Max Users in App (ram and cpu dependency)	150	500	1000
Max Typical Active Browsing Users	20	80	160
Max Typical Concurrent Transfers	10	30	60

Connector Agent Hardware Requirements

	Minimum	Mid-Range	High-End
CPU	ARM A8 Single Core @ 1ghz	ARM A9 Dual Core @ 1ghz	Intel Atom Quad Core @ 2ghz
RAM	256mb	512mb	512mb
Network	Single 1GbE LAN Port	Single 1GbE LAN Port	Dual 1GbE LAN Ports w/ Aggregated Links
OS	Linux based	Linux based	Linux based
Storage	7200rpm SATA Drives, < 10ms seek	7200rpm SATA drive(s), <10ms seek	10000rpm SATA drive(s), <7ms seek and/or SSD caching
Max Activations and/or Users	100	250	500
Max Logged in Users (ram and cpu dependency)	30	125	350
Max Typical Active Browsing Users	10	35	100
Max Typical Concurrent Transfers	5	15	30 (may be IO limited)
Expected CPU% Use at Max Typical	50%	50%	50%

View-Only Conversions

The advanced panel of the server administration contains a configurable property “Maximum concurrent view-only conversions”. This defines the maximum number of view-only conversions that may execute at the same time. When a user chooses to view an office document within the application, a conversion is necessary. The number of conversions that can happen at the same time is directly connected to the amount of CPU and RAM allocated to the server. Each “concurrent view-only conversion” requires 1 dedicated CPU core, and 1gb of RAM.

We recommend adding 1 CPU core and 1gb of RAM for each additional 1,000 users added to the system, depending on the frequency with which they are viewing documents within the application, and the size of the documents they are viewing.

Effect of RAM

The most important fundamental resource is RAM because several running processes are launched for data accumulation, proxying, data encryption, etc. A minimum of 2gb is required to run all needed services adequately. The maximum activations introduce a persistent RAM requirement, so a higher RAM total allows for more total activations/ users. Simultaneous transfers also require more RAM. A larger cache allows for a larger number of “active users”.

Effect of Disk IO

The server is not critically bound to drive IO, so most typical well-functioning NAS drive deployments will be adequate. The connector however which is responsible for fetching files from the local device is tied to the IO performance of the device - especially the seek time. SSD caching schemes will greatly improve it’s ability to deliver high numbers of files concurrently without overly slowing down the NAS’s performance.

Effect of CPU

The CPU is highly utilized for encoding/decoding of requests, so is directly related to the number of active users. It is also directly related to the number of high-speed transfers due to the active encryption. The CPU becomes especially important when dealing with 10GbE connections with clients located on the same high-performance network.

Effect of Network

The network is very important when dealing with a large number of concurrent transfers if one wants to maintain consistent local-network level performance. For the reasons described above, it's important to correlate the CPU with the network speed.

Clustering

When capacity becomes saturated, it is possible to deploy FileFlex in a clustered configuration. Supporting a clustered configuration requires dual networks, so it's important that such deployments have at least two network adapters. In a highly de-centralized deployment, the CPU and RAM become less important as the load is spread across several machines.

Virtualization

Supported Virtualization Platforms:

- VMware Workstation 11
- VMware Workstation 12
- VMware Workstation 12.5
- VMware ESXi 5.5 (vSphere)
- VMware ESXi 6.0 (vSphere)
- VMware ESXi 6.5 (vSphere)
- Oracle VirtualBox 5.1

Supported Platforms

The following is a list of verified supported platforms.

Product	OS	OS Type	OS Version
FileFlex Connector	Windows		Windows 7 32/64 bit
FileFlex Connector	Windows		Windows 8 32/64 bit
FileFlex Connector	Windows		Windows 8.1 32/64 bit
FileFlex Connector	Windows		Windows 10 32/64 bit
FileFlex Connector	Windows		Windows Server 2012 64bit
FileFlex Connector	OSX		OS X 10.13 High Sierra
FileFlex Connector	OSX		OS X 10.14 Mojave
FileFlex Connector	OSX		OS X 10.15 Catalina
FileFlex Connector	Red Hat Enterprise	Linux Enterprise: RPM Based on Fedora	RHE v6 64 bit RHE v7 64 bit
FileFlex Connector	CentOS	Linux Enterprise: RPM Based on Fedora Clone of Red Hat Enterprise	CentOS v6 64 bit CentOS v7 64 bit
FileFlex Connector	Ubuntu LTS Server	Linux Enterprise: DEB	Ubuntu LTS 14.04 64 bit Ubuntu LTS 16.04 64 bit
FileFlex Connector	Debian	Linux Enterprise: DEB	Debian v7 64 bit Debian v8 64 bit
FileFlex Connector	SUSE Enterprise	Linux Enterprise: RPM Based on OpenSUSE	SUSE Enterprise v11 64 bit SUSE Enterprise v12 64 bit
FileFlex Connector	Ubuntu Desktop	Linux Desktop: DEB	Ubuntu LTS 16.04 64 bit Ubuntu 16.10 64 bit Ubuntu 17.10 64 bit Ubuntu 18.04 64bit
FileFlex Connector	Fedora	Linux Desktop: RPM	Fedora v27 64 bit Fedora v28 64 bit

Product	OS	OS Type	OS Version
FileFlex Connector	Mint	Linux Desktop: DEB based on Ubuntu	Mint v17 64 bit Mint v17.1 64 bit Mint v17.2 64 bit Mint v17.3 64 bit Mint v18 64 bit Mint v18.1 64 bit
FileFlex Connector	OpenSUSE	Linux Desktop	OpenSUSE 42.1 64 bit OpenSUSE 42.2 64 bit

FileFlex Client App

Product	OS	OS Version
FileFlex Client App	Android	Android 6.0 Marshmallow (API 23)
FileFlex Client App	Android	Android 7.0 Nougat (API 24)
FileFlex Client App	Android	Android 7.1 Nougat (API 25)
FileFlex Client App	Android	Android 8.0 Oreo (API 26)
FileFlex Client App	Android	Android 9 Pie (API 28)
FileFlex Client App	iOS	iOS 12
FileFlex Client App	iOS	iOS 13
FileFlex Client App	Windows	Windows 7 32/64 bit
FileFlex Client App	Windows	Windows 8 32/64 bit
FileFlex Client App	Windows	Windows 8.1 32/64 bit
FileFlex Client App	Windows	Windows 10 32/64 bit
FileFlex Client App	OSX	OS X 10.13 High Sierra
FileFlex Client App	OSX	OS X 10.14 Mojave
FileFlex Client App	OSX	OS X 10.15 Catalina

FileFlex Web Client

Product	Platform Type	Platform	Browser Version
FileFlex Web Client	PC	Windows	Internet Explorer 11 and up
FileFlex Web Client	PC	Windows	70.0.1 (64-bit) and up
FileFlex Web Client	PC	OSX	Firefox 70.0.1 and up
FileFlex Web Client	PC	Linux	Firefox 70.0.1 and up
FileFlex Web Client	PC	Windows	Chrome 78.0.3904.108 and up
FileFlex Web Client	PC	OSX	Chrome 78.0.3904.108 and up
FileFlex Web Client	PC	Linux	Chrome 78.0.3904.108 and up
FileFlex Web Client	PC	OSX	Safari 13.0.3 and up
FileFlex Web Client	Mobile	Android	Android Mobile Browser 18.0.1025 and up
FileFlex Web Client	Mobile	Android	Puffin Mobile Browser 3.0 and up
FileFlex Web Client	Mobile	iOS	Puffin Mobile Browser 3.0 and up
FileFlex Web Client	Mobile	BlackBerry	BlackBerry Browser 10.2.0.1767 and up
FileFlex Web Client	Mobile	iOS	Safari Mobile Browser 3.5 and up
FileFlex Web Client	Mobile	Android	Chrome Mobile 18.0.1025 and up
FileFlex Web Client	Mobile	iOS	Chrome Mobile 19.0.1084 and up
FileFlex Web Client	Mobile	Android	Firefox Mobile 8.0 and up
FileFlex Web Client	Mobile	iOS	Firefox Mobile 8.0 and up
FileFlex Web Client	Mobile	Windows Phone	Internet Explorer Mobile 9.0 and up

