fileflex™ enterprise

Centralized vs Decentralized Cloud

qnext | fileflex.com
support@qnext.com

Executive Summary

The FileFlex decentralized cloud or edge computing architecture differentiates it from all other file remote access, sharing and collaboration platforms. Their dependence to duplicate and sync data to a central server cluster has resulted in compromises and issues such as an increased risk posture, privacy compromise, fragmented data, the need to manage limited subsets, technical complexity and high cost. Because of the tremendous productivity benefits the centralized structure offers, the market has accepted these compromises. However, the decentralized cloud architecture of FileFlex allows it to address the compromises and issues inherent to all competitive solutions at a lower cost. FileFlex improves the organization's security posture, allows access to all storage – not just subsets – ensures privacy, keeps the management of organizational files under organizational control, accelerates compliance to privacy regulations such as GDPR and HIPAA and leverages the organization's existing storage infrastructure to produce a disruptive low-cost model that can be applied to all storage.

Understanding the Centralized Cloud Architecture Used by All FileFlex Competitors

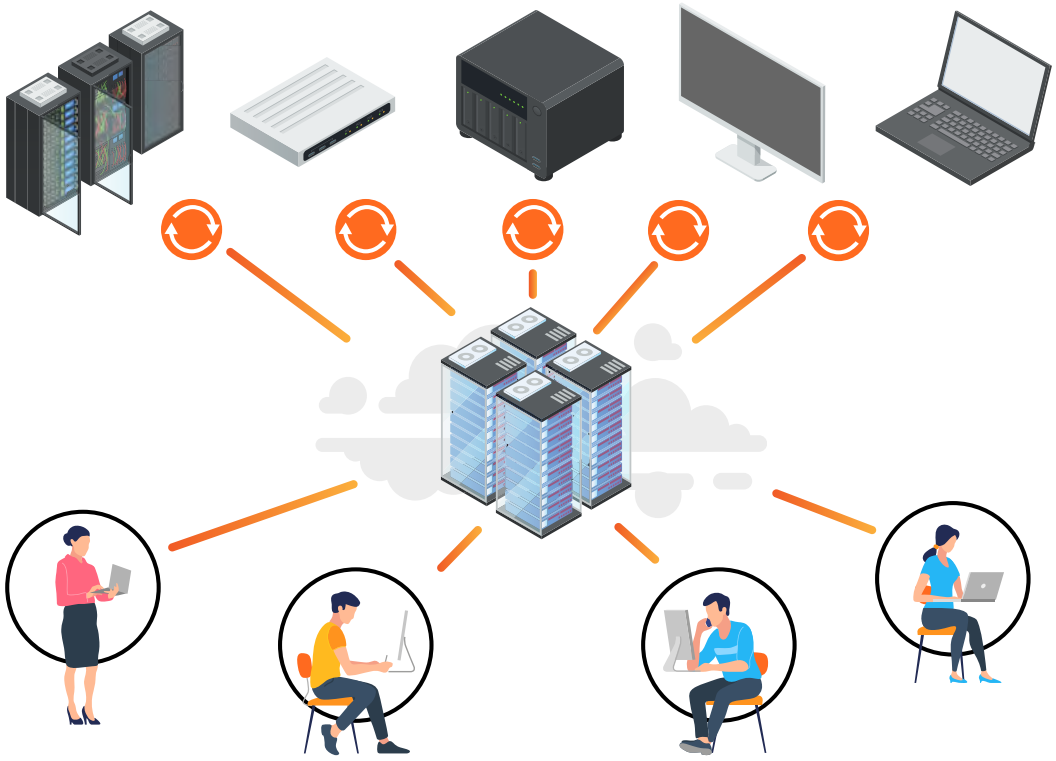


Diagram 1 - Centralized Cloud Architecture

Diagram 1 shows the basic architecture of traditional centralized cloud storage. It is the architecture of today's connected world used by all cloud providers whether public, private, EFSS, CCP or hybrid clouds, including Amazon, Google, Microsoft, Dropbox, Box, Citrix and Dropbox. In this model, hundreds, thousands or even millions of devices sync or duplicate a subset of their local storage to a central server cluster. Hundreds, thousands or even millions of users then connect to that server and access their files over the internet. Each user would have their own account on that server and files that they store or sync from their devices are then associated to their account.

Understanding Types of Centralized Clouds

There are many types of centralized clouds each with its own advantages and disadvantages, but all using a centralized server architecture. The following is a simplified understanding of the major categories of cloud storage services.

Public Clouds - When the central server cluster is located and operated by a third party like Microsoft or Google - and the user account is controlled by each individual user it is called a public cloud. This is the lowest cost type of cloud and entry level accounts are free of charge. Since the account is under the control of the individual user, the organization has no control or visibility over that content once it has been moved there.

EFSS or CCP - If the server is located and operated by a third party but user account is controlled by the organization it is called an Enterprise File Sync and Share (EFSS) service. It is also called a Content Collaboration Platform (CCP). The EFSS cloud is simply a public cloud with organizational control.

On-Premise EFSS – An on-premise EFSS service is when the server is located on the organization's premises, but the service uses the software of an EFSS provider.

Private Cloud - When the central server cluster is under the control of an organization, located on their own premises and behind their firewall, this is called a private cloud. Since the organization must build and operate the server cluster and the cloud software themselves, it is the most expensive and difficult type of cloud to operate.

Virtual Private Cloud - When the central server cluster is under the control of an organization, but is located in a third-party data center, it is called a virtual private cloud. By locating the server cluster in a third-party data center an organization can reduce costs and increase their security and reliability.

	Public Cloud	EFSS	Virtual Private Cloud	Private Cloud
Account Countrol	User	IT	IT	IT
Location of Data	Third-Party Datacenter	Third-Party Datacenter	Third-Party Datacenter	On-Premise Server
GRC (Who Operates the Server)	Third-Party	Third-Party	IT	IT
Coverage	Subset	Subset	Subset	Subset
Privacy (Can a Third Party Secretly See My Data?)	Yes	Yes	Yes/No	No
Type	Public	Public	Private	Private
Cost	Inexpensive	Moderate	Expensive	Very Expensive

Table 1 - Types of Cloud Services

Types of Cloud Environments

Hybrid Cloud – A hybrid cloud environment is when an organization uses a combination of public/EFSS cloud and private cloud. For example, they may store their confidential and sensitive information in a private cloud, but in order to reduce costs, store normal business information in a public or EFSS cloud. This is a hybrid cloud environment.

Multi-Cloud – A multi-cloud environment is when an organization uses the cloud facilities and services of multiple vendors. For example, for various reasons they may use Amazon S3, Microsoft Azure and IBM Cloud. They then have a multi-cloud environment.

Issues Inherent to the Centralized Cloud Architecture Used by All FileFlex Competitors

Since cloud storage services all use the centralized server architecture they all have the following issues and compromises that are inherent to the architecture itself.

Duplication, Increased Threat Surface, More Complicated Storage Structure - With all cloud types – public, EFSS, private and virtual private clouds – users duplicate a subset of their files to the centralized server cluster so that those files can be accessed over the internet. This creates duplication and version control issues. Since each server will typically have both a near-line and off-line backup and may be replicated in other geographies to provide better global access there will be multiple copes of each file stored. Each copy made increases the threat surface of the organization and creates a more complex storage structure. This inherently increases the risk posture of the organization.

Subsets - Since many users and devices sync or store information on the centralized server cluster and because that server has limited storage, only a subset of an organizations overall data can be stored. That means that users will have to manage their allotment and often critical data will not be on that server and is unavailable. For example, an organization may have 1000 terabytes of overall data storage across all devices, users and locations. If they have 100 terabytes of cloud storage, then 900 terabytes of data are inaccessible at any given time due to the fact that not all storage has cloud functionality.

Resource Intensive - The constant syncing from all users and all their devices ties up multiple CPU cycles and bandwidth. It is very resource intensive requiring multiple servers, load balancers and facilities that all must be managed and secured.

Expensive - The centralized server model – depending on the scale – requires an expensive data center - multiple servers, storage arrays and supporting equipment such as UPS, backup generators, cooling, etc. The data center must be maintained by trained technical staff and it must be secured against malware, hackers, fire, theft, natural disaster, outages and human error. This is all to support the accessibility of data that is essentially a duplication making it expensive.

Additional Issues Inherent to Cloud Architecture Used by EFSS & Public Cloud FileFlex Competitors

Privacy

Not all EFSS products are created the same when it comes to security and that is the real problem. Some public cloud vendors like Microsoft and Google adopt very strong security practices that are equivalent or better than those found in corporate IT departments - some do not. However, even though some may be very secure and some not, none of them can protect the privacy and confidentiality of the information stored on their servers. From a privacy perspective it is never a good idea to give your confidential information to someone else. This information can legally be secretly accessed and exfiltrated by the cloud provider, by law enforcement and in some cases, by foreign powers.

Secret Exfiltration from Third Parties – The cloud provider is required by law to make sure that you are not using their platform for illegal activity. They must, and do inspect your files for copyright infringement, child pornography, terrorism and money laundering for example. In any case, they have the right to secretly inspect your files at their discretion for any reason they determine.

Secret Exfiltration from Law Enforcement - What about law enforcement trying to access your data? With EFSS and public cloud storage you may not know that the provider was served a subpoena, warrant or security order. In fact, the provider may be prohibited by law from telling you.

Although nearly every provider's terms read differently, one thing remains the same. They all tell you explicitly they must and will comply with legal requirements from governments, security agencies and law enforcement (to secretly access your files) and are not responsible for any loss you experience.

Secret Exfiltration from Foreign Powers - With the passing of the Cloud Act, U.S. law enforcement can serve an SCA "warrant" to cloud providers where recipients such as Google, Amazon or Microsoft are obligated to turn over evidence wherever located – even if it is stored on a server located in another country. Since SCA warrants are served in secret directly to the cloud provider and your cloud provider is prohibited from informing you that they have

received a warrant to hand over your data, you are depending on them to defend your privacy. If for whatever reason they fail to do so, your data will be exfiltrated without your knowledge. The sole remedy is for the cloud provider to ask a court to quash or modify the warrant. To quash or modify the warrant, all 3 of the following conditions must be met: (a) the target is not a U.S. person; AND (b) compliance would conflict with the law of the country where the data is stored; AND (c) the court conducts a "comity" analysis and concludes that, on balance, disclosure isn't warranted. If the data requested in your cloud storage is for a U.S. person or if the target of the request is a non-U.S. person but your own country does not have any specific privacy law to protect that data, then you have no protection. Finally, even if the request is for data on a non-U.S. person and it violates the privacy laws of your local government but the U.S. based court determines that U.S. law enforcement really needs it, then your data will be exfiltrated.

Second the bill is reciprocal in nature as it would allow the Executive Branch to enter into "executive agreements" to allow qualified foreign governments with restrictions, to acquire data of their own citizens wherever located including if stored on servers located in the U.S., without regard to U.S. law or the U.S. constitution.

In short, under certain circumstances, foreign governments can access data stored in public cloud services regardless of where the data is physically located around the globe, potentially circumventing local regulations. And the European Commission isn't sitting idly by. It is readying its own legislation called the E-Evidence Directive to enable EU member countries the same jurisdictional reach as the U.S.

Governance, Risk Management and Compliance (GRC)

With growing pressure to empower employees, associates and customers with the latest mobile technologies and BYOD, governance, risk management and compliance (GRC), and who operates and controls the centralized server cluster is vital for an organization's security strategy. The problem using the cloud and EFSS means your 'latest technologies' can quickly become a compliance headache because the actual compliance and management is outside of your control.

Understanding the FileFlex Difference – The Decentralized (Edge) Cloud Architecture

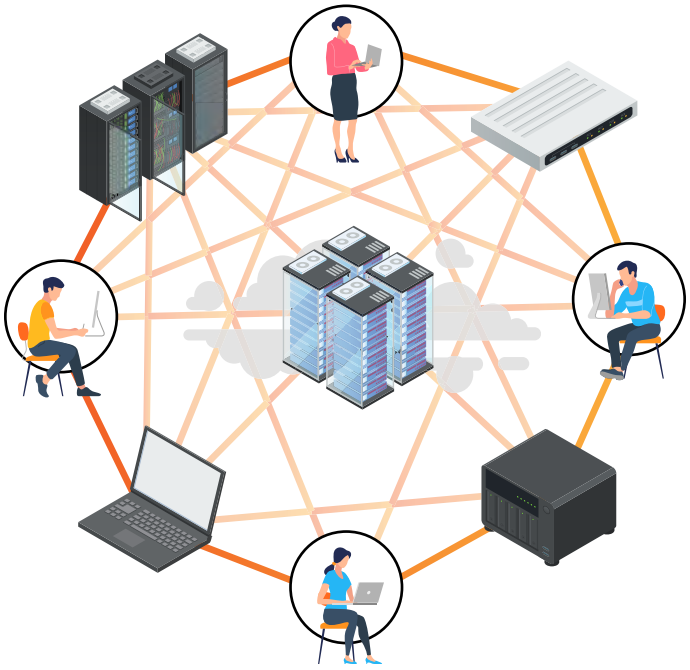


Diagram 2
The Decentralized Cloud Architecture of FileFlex

FileFlex is differentiated from all other competitors in that it uses a decentralized or edge computing architecture instead of the centralized cloud model. It addresses all of the compromises and issues of the centralized cloud model listed above. Instead of transferring and storing data in a central data center located miles away from connected devices, edge computing is a revolutionary technology that moves processes and storage to the device at the edge of the network to make the cloud more efficient. It is the same type of technology that will power the Internet of Things (IoT) and the coming hyper-connected world that will be enabled by 5G technology.

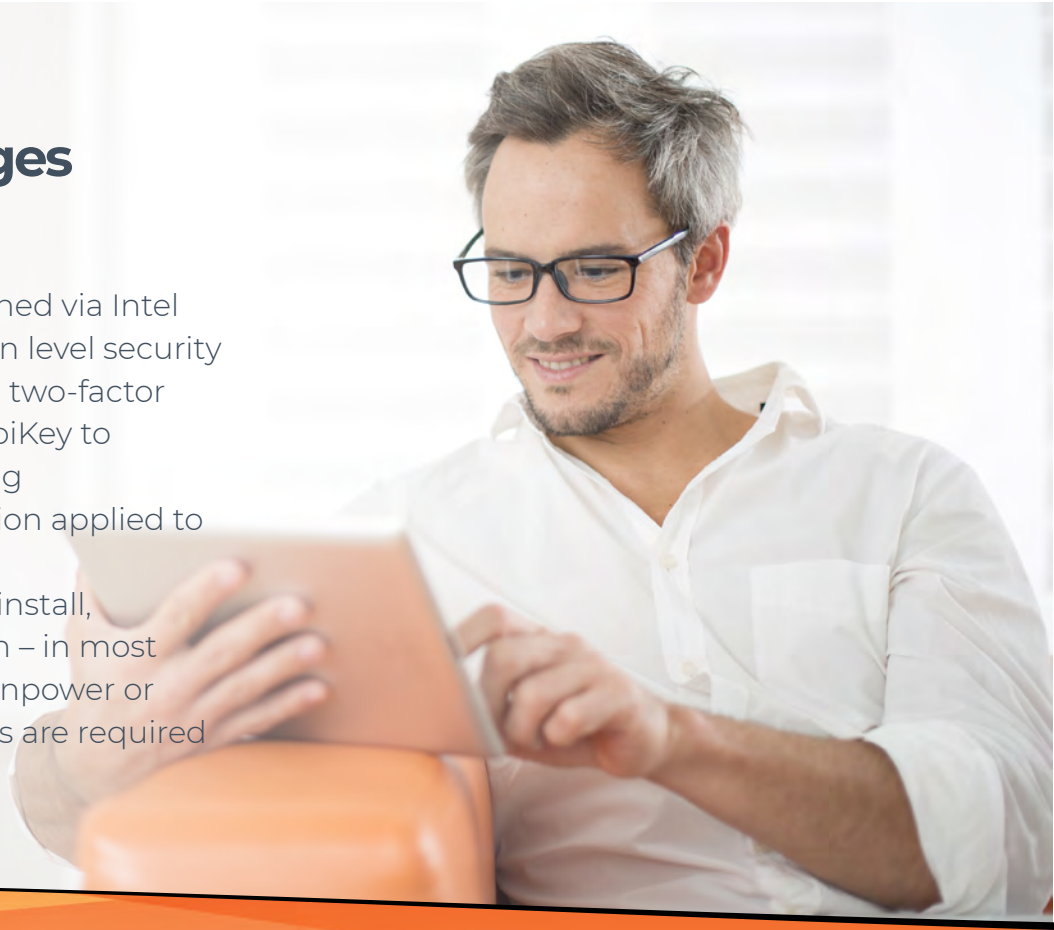
FileFlex leverages the CPU power and storage of the end-point devices who communicate directly with each other. The central server acts like a switchboard to facilitate a hybrid point-to-point connection and as a policeman to enforce policies. Data is stored in source locations which all now have cloud functionality of remote access, sharing, streaming, collaboration and file management. Privacy and confidentiality is protected by keeping data in source locations, on-premise, behind the corporate firewall, on corporate storage assets, in specific geographic regions and access controlled. Also, with this technology users can access all storage not just a subset that is duplicated to a central server. And because it leverages the existing storage and servers the organization already owns, organizations do not have to build a private cloud or subscribe to an expensive EFSS service making it is the lowest cost model.

Advantages of a Decentralized Cloud (FileFlex)

- All files from the entire organizational storage infrastructure can be remotely accessed, shared and collaborated, even from multiple locations – not limited to subsets
- No duplication to third party servers or secondary locations – reduces the threat surface and simplifies the storage structure for a reduced risk posture
- Governance, Risk Management and Compliance (GRC) under organizational control
- Files can be kept on-premise, behind the corporate firewall, on corporate assets, in specific geographic locations and access controlled to protect privacy and prevent secret exfiltration from third parties, law enforcement and foreign powers
  - This also accelerates compliance with GDPR, HIPAA and all other privacy regulations
- Leverages existing storage infrastructure and servers for the lowest cost model

Other Advantages of FileFlex

- Can be platform hardened via Intel CPU for silicon-to-silicon level security
- Supports U2F universal two-factor authentication and YubiKey to protect against phishing
- Is a software-only solution applied to existing storage
- Very easy and quick to install, configure and maintain – in most cases no additional manpower or infrastructure resources are required



fileflex.com
support@qnext.com

Competitive Product Overview

Private Cloud Platforms

With private cloud-based platforms, files are synced and/or duplicated to a cloud server/ storage that the organization owns and controls.

Suppliers

ownCloud, FileCloud and Einstein

FileFlex Differentiation

- Private clouds duplicate and/or sync data to a cloud server that the organizations owns which;

  1. Increases the threat surface
  2. Complicates the storage infrastructure

  This increases the threat posture of the organization. FileFlex accesses files from their source locations without creating duplication. This reduces the threat surface and simplifies the storage infrastructure to lower the organization's threat posture.

- Private clouds allow a user to access and share files stored on a subset of the company's storage. FileFlex makes all corporate data accessible by enabling any server, notebook, desktop, SAN, NAS, public, private or virtual private cloud to be available.

- Private clouds are very expensive as they require customers to build, maintain and pay the entire cost of the data center. FileFlex leverages existing servers and storage so that no additional hardware investment is required.

- Due to their high cost, private clouds typically restrict the number of users and how much space each user is allowed. With the low cost of FileFlex, there is no need for storage or user restrictions. All data is available to all users subject to Active Directory permissions and IT control.

- Private clouds require a very high level of technical expertise to deploy and maintain such that they are attractive to only the largest of enterprises and out of reach for SOHO and SMB businesses. Users may also require product training. FileFlex requires very little to no technical expertise or training.

EFFS, Hybrid Cloud Platforms

EFSS clouds are simply a public cloud with IT oversight. They can range from the EFSS server and storage hosted by the EFSS provider (cheapest) to the EFSS server and storage customized and hosted by the client organization which is essentially a private cloud (most expensive) - see private cloud analysis above.

Hybrid clouds use a combination of on-premise cloud storage and business-grade EFSS storage depending on the customer's need for data privacy. It can range from 100 per cent on-premise for maximum control (a 100% private cloud) to a sliding portion of non-critical data to EFSS storage to reduce costs.

Suppliers

Accellion Kiteworks, Acronis Access, VMWare Secure Content Locker, Egnyte, Syncplicity, IBM Aspera, Novel Filr, BlackBerry Workspaces (WatchDox), Tresorit, Box, Dropbox for Business, Google Drive for Work and OneDrive for Business.

FileFlex Differentiation

FileFlex enjoys the same advantage as it does over private clouds (see above) plus:

- Since EFSS and hybrid platforms may require uploading some files to a third-party data center, the solution inherently introduces privacy and security risks such as breaches and outages. Even the likes of Dropbox have been breached and Google Drive, OneDrive and Amazon have all experienced service outages.
- Uploading data to a third-party data center also raises unresolved issues of legal jurisdiction. Is the data under the jurisdiction of where the physical server is located, where the host company is incorporated or where the user is located? FileFlex resolves issues of legal jurisdiction and data residency as files, including meta data, can be stored easily on-site and in a specified jurisdiction.
- EFSS providers cannot ensure the privacy of confidential documents. All files stored with EFSS providers are subject to potential secret exfiltration from the cloud provider, in-country law enforcement and potentially from foreign powers. FileFlex addresses privacy concerns as all data can be on-premise, under the control of users behind their firewall with all access logged. Secret exfiltration is not possible.

- EFSS clouds limit personal and business storage space making users and IT pick and choose what to sync to the cloud. FileFlex makes all corporate data accessible. As a result, syncing data is no longer an issue.
- EFSS and hybrid clouds use compression to speed data transfers. This can cause quality degradation issues. With FileFlex there are no uploads required and files are accessed without compression.

Personal Cloud Platforms

Suppliers

Tappin, Polkast, WD MyCloud, QNAP FileStation/QFile, Synology FileStation/DSFile, ASUS AiCloud and Netgear ReadyCloud.

FileFlex Differentiation

- Personal clouds provide remote access to either a PC or a NAS and nothing else. FileFlex provides remote access to all devices and storage that are attached to the same network as the PC or NAS and transforms that personal device into a gateway for remote access to the server, any other server attached storage such as a SAN, DAS, cloud or other NAS, and every PC and laptop on the same network.
- Personal clouds provide remote access to users with device credentials only and files are shared by file downloading via a link. Once a link has been issued, it is difficult to control the future distribution of that link and/or unintended and unauthorized downloading of the file. Also, with every share and download, a duplicate copy of the file is created. To disable sharing, the link must be disabled affecting everyone who has that link. Sharing with FileFlex, however, is via access to source documents in their original locations to intended email contacts only.
- Personal clouds allow streaming of movies, videos and music only to users with device credentials. Family, friends and contacts who are not device users cannot stream media. The user must share a link to allow the recipient to download and then play the file. They cannot stream directly from the source location. FileFlex allows any user contact with permission to stream content directly from the source location.

fileflex™ enterprise

qnext

fileflex.com
support@qnext.com