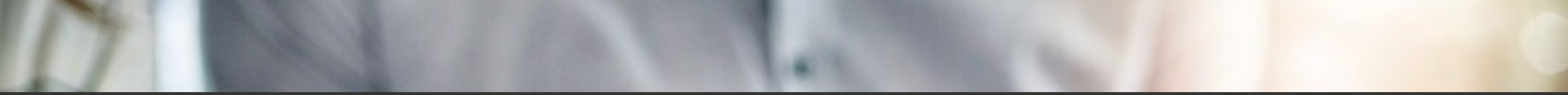
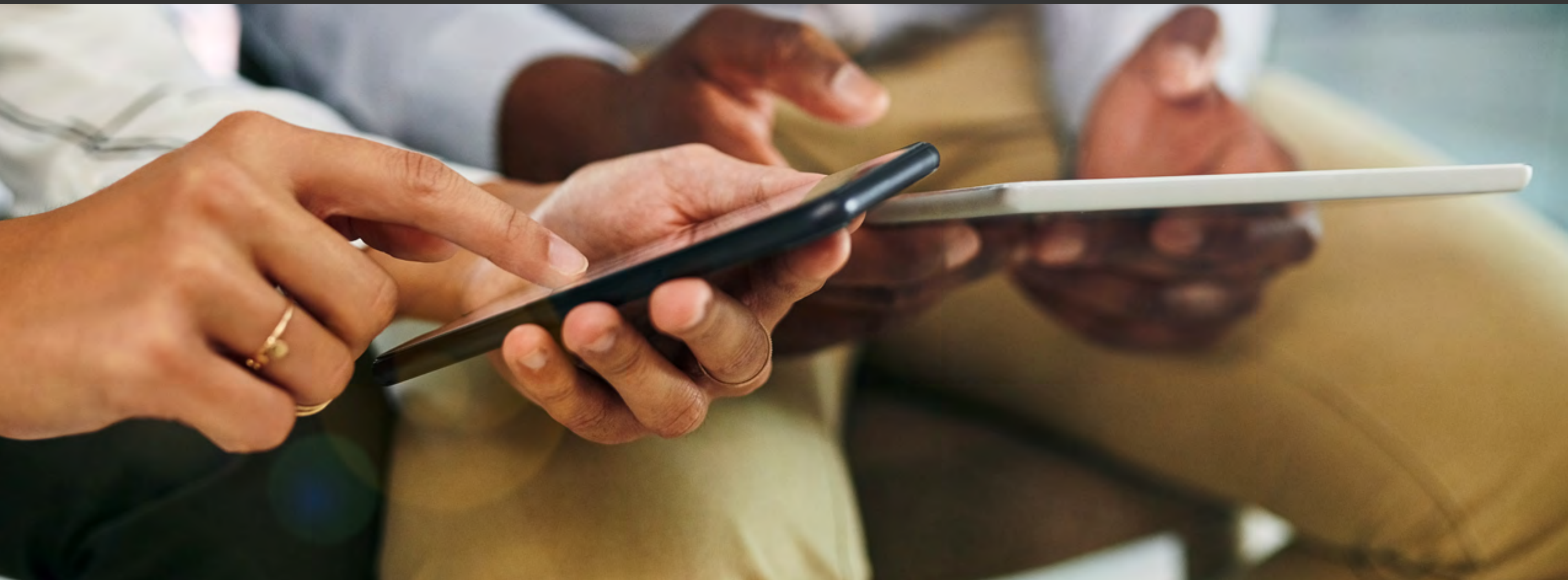
fileflex™
enterprise

How to Make Your Multi-Cloud and Infrastructure-as-a-Service Environment Easier for Your Users



Infrastructure-as-a-Service and a multi-cloud environment adds layers of complexity to your IT infrastructure. IT has learned to handle the complexity and the vendors have provided the tools to manage it, but what about tools for the end-users. Sadly, these are lacking. This paper starts with a primer on multi-cloud, the needs of your end-users, a look at security concerns, the issues of addressing end-user needs through a virtual private cloud implementation and finally using the decentralized or edge architecture of FileFlex Enterprise to provide secure remote file access, sharing and collaboration of your multi-cloud while improving your security posture and allowing access to all storage.



> **“Multi-cloud providers are Infrastructure-as-a-Service platforms. They essentially act like your own on-premise server/storage infrastructure, except that they are located and hosted in a third-party datacenter – like Google, Amazon of Microsoft.”**

Most organizations today use multiple Infrastructure-as-a-Service providers and operate in a multi-cloud environment. According to RightScale, the average enterprise uses just over 3 public clouds and just under 4 private clouds and that the use of multiple cloud providers is the norm. The problem is that multi-cloud has added layers of complexity to an IT infrastructure. Although IT is petty good at handling the technical complexity, tools to help end-users are sadly lacking. How can you make your multi-cloud and Infrastructure-as-a-Service storage easier to navigate and operate for the average user?

What is the Multi-Cloud?

In a recent Forrester survey, respondents identified with the phrase “Using multiple public and private clouds for different application workloads” to describe and define what a multi-cloud environment is. It included using multiple cloud platform providers (IaaS) (32%), using both public clouds with traditional on-premise systems (23%) and using multiple public clouds simultaneously for different workloads (14%).

We should note here the difference between ‘multi-cloud’ and hybrid cloud’.

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 Infrastructure-as-a-service (IaaS) vendors. For example, for various reasons they may use Amazon AWS, Microsoft Azure and Google Cloud. They then have a multi-cloud environment.

Multi-Cloud Statistics

$32.4 BILLION

According to Gartner, the worldwide total amount spent on IaaS

31.3%

The increase over 2017

81%

The number of public cloud users that choose two or more providers

Source:
https://www.gartner.com/en/newsroom/press-releases/2019-07-29-gartner-says-worldwide-iaas-public-cloud-services-market-grew-31point3-percent-in-2018

Why Do Most Organizations Have a Multi-Cloud Environment?

Shadow IT – For many organizations, they arrived at the multi-cloud because various business units adopted it independently of the IT department – in other words due to ‘shadow IT’. According to McAfee, the average enterprise uses 31 cloud services.

Mergers, Acquisitions and Regulations – For some organizations, they inherit IT infrastructure when they go through a merger or acquisition. For others, they have facilities in multiple geographic locations that must comply with local data residency regulations – such as GDPR in Europe – which may have led to the utilization of local multiple cloud providers.

> **“Most organizations adopt a multi-cloud strategy out of a desire to avoid vendor lock-in or to take advantage of best-of-breed solutions”**
>
> - Gartner VP analyst Michael Warrilow

More than half of firms running containers today are doing so in "hybrid mode."

53%

amount of containers run in hybrid mode - both on-premise and at least **1** cloud

23%

amount of containers run in hybrid mode - both on-premise and at least **2** clouds

Source:
https://www.stackrox.com/kubernetes-adoption-and-security-trends-and-market-share-for-containers/

Control – Ultimately IT is responsible for your IT platform. One reason IT purposely adopts multi-cloud is that they do not want to be held hostage to a particular cloud provider. Cloud providers also generally provide some advantage that differentiates them from their competitors and make their platform 'sticky'. In order to take advantage and full functionality of particular workloads but also have leverage over the cloud provider, most large organizations willfully choose a multi-cloud strategy.

Speed – Sometimes an organization may choose multiple cloud providers that are geographically close to the locations that need services in order to get better performance. For example, for performance reasons a multinational organization with offices in North America and Japan will want cloud providers in both geographies.

Protection against outages and downtime – All cloud platform providers have outages and no IT executive wants to see facilities down because their cloud provider is down. Just like most have multiple internet providers to keep things running when their provider has an outage, many will have multiple cloud platforms to keep their organization productive when their cloud platform is down.

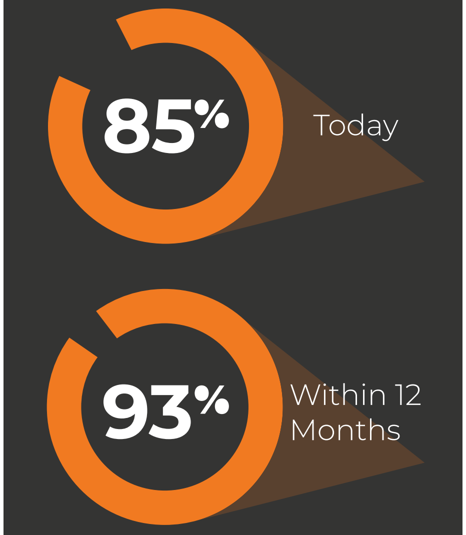
Make Your Multi-Cloud Easier for Your Users

Most IT leaders have brought in the tools that they need to manage their multi-cloud environment from a technical perspective. They have bought the deployment, migration and management tools they need for provisioning and orchestration; service request management; inventory and classification; monitoring and analytics; cost management and resource optimization; cloud migration, backup and disaster recovery; and identity, security and compliance from vendors such as Flexera (RightScale), Scalr, Embotics, Morpheus Data and even Google's Anthos. However, tools to help users navigate and use this complex environment are sadly lacking.

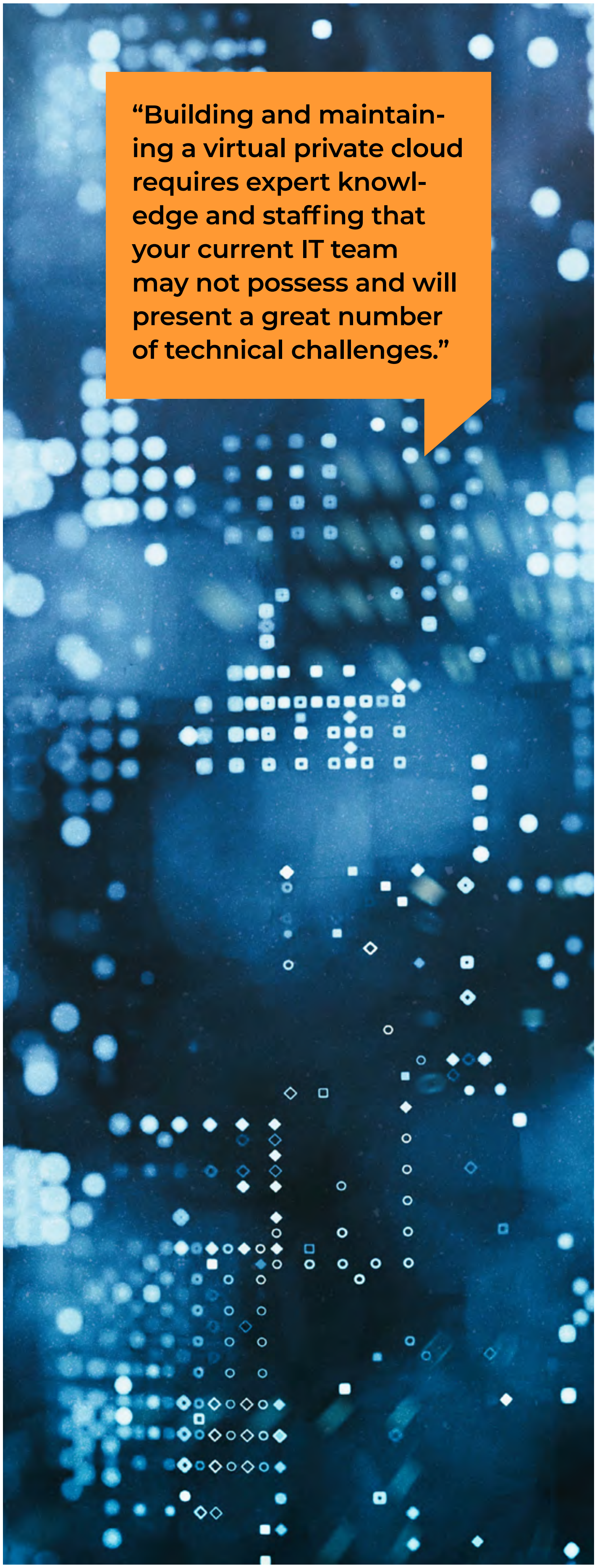
Remote access, sharing and collaboration - Multi-cloud providers are Infrastructure-as-a-Service platforms. They essentially act like your own on-premise server/storage infrastructure, except that they are located and hosted in a third-party datacenter – like Google, Amazon of Microsoft. As such, they generally do not have any native remote access, sharing and collaboration capability.

Cut, copy, paste and general file management – Multi-cloud providers have no end-user file management capability like cut, copy, paste, rename etc. They have management utilities for IT such as AzCopy, AWS Explorer and Google Cloud Shell, but are not equipped for end-users.

Multicloud as Percent of Cloud Adopters



Source: https://www.cisco.com/c/dam/global/en_uk/solutions/cloud/overview/cloud_business_cloud_advisor_infobrief_eng_FY18Q3.pdf



> “Building and maintaining a virtual private cloud requires expert knowledge and staffing that your current IT team may not possess and will present a great number of technical challenges.”

But What About Security?

In the same way that having a multi-cloud architecture means securing a multi-cloud architecture, having easy end-user access to your multi-cloud storage means securing their access.

To be successful in that, you'll need to develop a multilayered strategy that makes use of technologies that secure both applications and data. You'll need to consider controls for user access that work across cloud boundaries. Normally, it is the responsibility of the cloud provider to secure their infrastructure, and they will or should be able to provide you some of the capabilities you need in order to protect your data while it’s in their facility. But what about the third-party applications you are using in that infrastructure such as providing remote access to cloud storage for your users. Those applications need security capabilities such as multi-factor authentication, encryption, virus scanning, active directory integration, SSO and identity and access management, device authentication, credential protection and an activity log for incident management.

What About Building a Virtual Private Cloud

One way to allow end-user access to your multi-cloud or Infrastructure-as-a-Service storage is to use it to build a virtual private cloud. A private cloud is cloud storage for remote access and sharing that you build on your on-premise infrastructure behind your firewall that is for the use of your own organization alone. A virtual private cloud is when you host your private cloud on your Infrastructure-as-a-Service provider instead. All private clouds, no matter who they are, use the same basic architecture. They all sync or copy to a centralized cloud server cluster. In this case that central server cluster is located with the Infrastructure-as-a-Service provider. In this model, hundreds or even thousands of devices sync or duplicate a subset of their local storage to the central server cluster. Hundreds or even thousands 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.

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 Infrastructure-as-a-Service cloud storage, then 900 terabytes of data are inaccessible at any given time due to the fact that not all storage has cloud functionality.

Technical Challenges

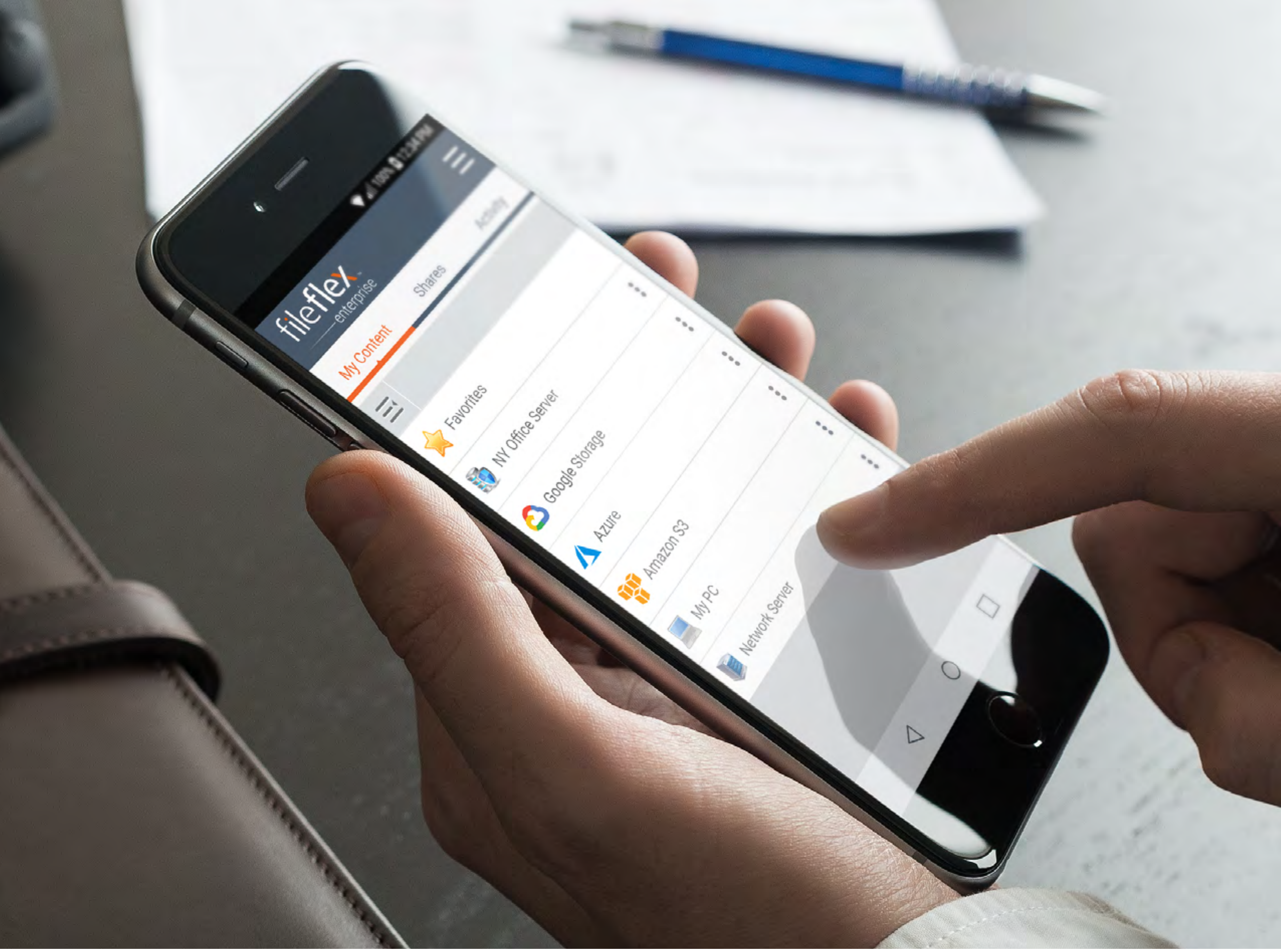
Building and maintaining a virtual private cloud requires expert knowledge and staffing that your current IT team may not possess and will present a great number of technical challenges.

If you do not have accomplished private cloud experts on your team—and there are not too many of those out there—it will be extremely challenging to get your virtual private cloud project off the ground. Your IT department needs to be big enough with enough expertise and if you do not do it right at the early stages of a deployment, things might break later. This might impact your ability to build the private clouds with the precise capabilities you need and meet your timelines for milestones during the project.

24%

rank the ability to ensure the security of workloads across platforms considered the top challenge to that freedom of movement in multi-cloud environments.

Source:
https://www.gartner.com/smarterwithgartner/why-organizations-choose-a-multi-cloud-strategy/



> **“FileFlex is differentiated from private cloud alternatives 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.”**

Use FileFlex to Make Your Multi-Cloud Easier for Your Users

FileFlex is differentiated from private cloud alternatives 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.

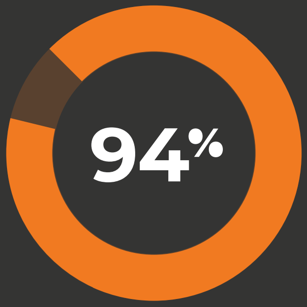
FileFlex leverages the CPU power and storage of the end-point devices who communicate directly with each other. The central server acts like a switchboard to facilitate a hybrid point-to-point connection and as a policeman to enforce policies. Data is stored in source locations which all now have cloud 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 your Infrastructure-as-a-Service storage, organizations do not have to build a virtual private cloud.

In the same way that you use the decentralized cloud technology of FileFlex for remote access, sharing, collaboration and management of your on-premise storage, you can use FileFlex for your Infrastructure-as-a-Service multi-cloud storage. FileFlex actually makes it very simple and puts all your cloud platforms and on-premise storage under a single-pane-of-glass – or on the same dashboard. It simply treats each cloud provider as a content repository. Use FileFlex to add the following functionality to your multi-cloud and Infrastructure-as-a-Service providers:

1) Add end-user remote access capability to your multi-cloud

FileFlex provides users remote access to the files and folders stored on your multi-cloud and Infrastructure-as-a-Service environment. Access can be from a Windows, Mac or Linux computer; Android, iOS, BlackBerry or Windows tablet or smart phone; or any internet connected kiosk. The access to all storage is from a simple dashboard.

Multicloud Deployments are Now the Norm

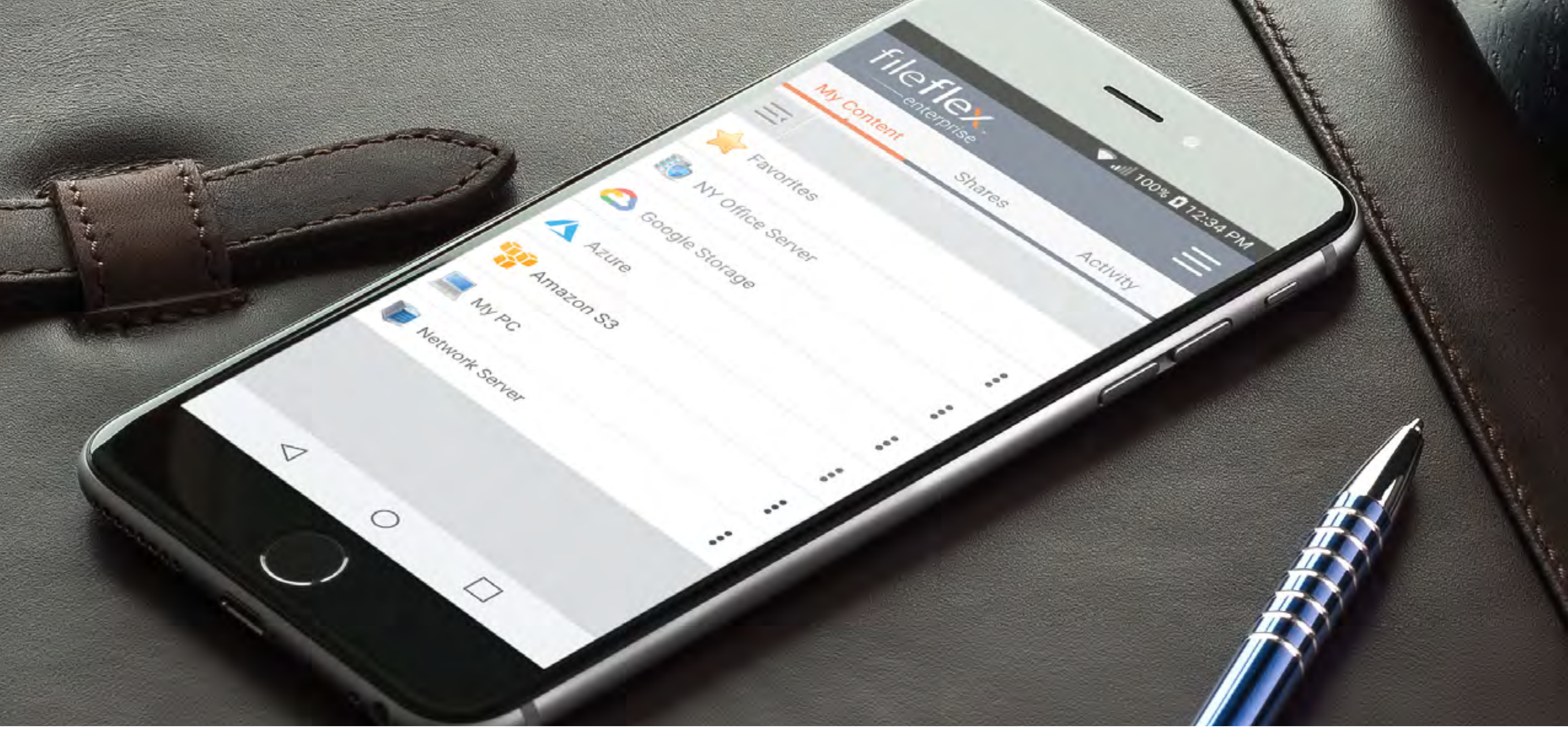


of cloud adopters have multiple types of cloud deployment options

working with at least four vendors

of cloud adopters work with at least ten cloud vendors

Source:
https://www.cisco.com/c/dam/global/en_uk/solutions/cloud/overview/cloud_business_cloud_advisor_infobrief_eng_FY18Q3.pdf



2) Add robust file sharing to your multi-cloud

Remotely share files stored on your multi-cloud or Infrastructure-as-a-Service cloud without having to sync, move, duplicate or upload them to a public or EFSS cloud by providing shared access to where they are saved. FileFlex does not use sharing links that can be forwarded or copied to social media. Instead it is permission-based access to source locations. The edge-computing technology of FileFlex makes files and folders shared act like an extension of the recipient's local device. There are no storage limitations, no file size limits, no quality degradation (no compression) and no complicated IT type setup requirements for the sharing of files.

"FileFlex provides users remote access to the files and folders stored on your multi-cloud and Infrastructure-as-a-Service environment. It puts all your cloud platforms and on-premise storage under a single-pane-of-glass"

3) Add remote file management to your multi-cloud

Use any internet connected smart phone, tablet or secondary computer to remotely cut, paste, copy, delete, rename, move and organize any document stored on your multi-cloud or Infrastructure-as-a-Service environment. Even cut, copy and paste files between cloud providers or between your on-premise storage remotely. Users don't have to be at home or in the office to organize files, they can keep things organized from anywhere. Supports Amazon S3, Microsoft Azure and Google Storage.

4) Turn your multi-cloud into a powerful content collaboration platform

Enables productivity and content collaboration for individuals and teams inside and outside the organization from multi-cloud or Infrastructure-as-a-Service source locations without duplicating

or syncing confidential content to a secondary location or a third-party server. Activity tracking, audit trail, version control, file locking, a unified workflow across devices, and simple, secure access make teams more productive and protects organizational information.

"FileFlex allows you to set your sharing options so that downloading is not permitted. As a result, no unauthorized copies are made of your files and you maintain control over the privacy of the files that are shared from your multi-cloud or Infrastructure-as-a-Service storage."

5) Add media streaming to your multi-cloud

FileFlex allows you or any contact to stream media files from your multi-cloud and Infrastructure-as-a-Service storage. This allows the consumption and sharing of massive collections of digital media right from this environment in a way that is simply not possible using traditional public, private or EFSS cloud technology. Users don't need to download – They stream directly from your IaaS storage.

6) Add automatic backup of photos and videos to your multi-cloud

Automatically back up the photos and videos from as many smart phones and tablets as you want to your multi-cloud or IaaS storage. You can even set FileFlex to only backup when connected via WiFi so as to not use up cellular data.

7) Add enhanced security to your multi-cloud

FileFlex adds AES 256 encrypted hybrid point-to-point communication, optional double-encryption, U2F universal two-factor authentication, device authentication, virus scanning, single sign-on (SSO) and active directory integration for a much lower risk posture when using multi-cloud or Infrastructure-as-a-Service cloud providers.

8) Add activity logging and enhanced incident management to your multi-cloud

FileFlex logs all activities – even for in-app activities via multi-clouds and Infrastructure-as-a-Service clouds – for audit and regulatory compliance issues. Know what files have been shared from your Amazon S3, Microsoft Azure and Google Cloud services and when. Know who shared what files and when. Know who accessed shared files and when, and know who downloaded shared files and when. For operations and incident management the audit log of activities can be exported and then imported using the common import protocols to the most popular risk management systems.

9) Enhance the privacy of your multi-cloud and prohibit downloading

FileFlex allows you to set your sharing options so that downloading is not permitted. As a result, no unauthorized copies are made of your files and you maintain control over the privacy of the files that are shared from your multi-cloud or Infrastructure-as-a-Service storage. View-only sharing for the consumer version of FileFlex applies to media files such as photos, videos, music and movies only. In FileFlex Enterprise, FileFlex allows for view-only sharing for all files as well as media files, including business documents such as Word, Excel, PowerPoint and Adobe PDF files. Thus, when your cloud storage complies with data residency requirements and is accompanied with appropriate user behavior, FileFlex can be used for the sharing of Personally Identifiable Information (PII) and aid compliance to privacy regulations such as HIPAA and GDPR because downloading of PII can be prohibited.

10) Add IT control over user activity in your multi-cloud

Users of FileFlex Enterprise can download the free FileFlex server and IT is in complete control over secure remote access and sharing and user activity in your multi-cloud and Infrastructure-as-a-Service storage. IT control who is provisioned, who they can share with, how much bandwidth they can consume and what content and storage they can access. It is easy to deploy, easy to integrate, scalable, easy to manage, supports multiple locations and all storage options. And they can have it up and running in just a couple of hours.

11) Use FileFlex for as a migration tool

Not only is FileFlex an easy tool to provide file management between cloud platforms for your end users, you will find it a great tool that IT can use for both data migration between on-premise storage and servers and their cloud providers and even from one cloud platform to another. From a single dashboard, you can cut, copy, paste, delete and rename files or folders of any size using the hybrid point-to-point edge technology of FileFlex. You do not have to use the cloud providers proprietary migration tools or download then upload to an intermediate location first. File size does not matter – the files and folders can be huge. You are only limited by your own storage capacity.

> **“Not only is FileFlex an easy tool to provide file management between cloud platforms for your end users, you will find it a great tool that IT can use for both data migration between on-premise storage and servers and their cloud providers and even from one cloud platform to another."**