qnext

Data Sovereignty: The New Priority

Preventing Possible Data Exfiltration Inherent to Cloud Storage Solutions

Executive Summary

As more employees work remotely, they need access to files located on the company network, which, in most cases, exist behind a firewall. To solve this problem, organizations often resort to storing files in enterprise-grade public cloud services for quick access across devices. But that surfaces numerous problems with data sovereignty—not only can cloud providers secretly access files, nation states, through new legislation, are increasingly extending their legal jurisdiction over cloud servers that are outside of their own geographic territories. In short, when files have been uploaded to a public cloud service, there is no visibility or control over data exfiltration and the concept of protecting privacy via data residency is no longer necessarily valid.

Compounding this issue, organizations have no idea if files have been accessed without its authorization. And although private clouds can potentially mitigate some of these problems, they are expensive to implement, manage, and configure. FileFlex is a revolutionary approach to solving the problems of providing remote file access while maintaining tight control over data sovereignty and preventing data exfiltration.

This whitepaper explores the challenges associated with remote file access, mitigating data exfiltration, and explains how FileFlex can ensure data already under your Governance, Risk Management, and Control (GRC) framework stays that way.

The Underlying Issue with Remote File Access

Jim fiddled with his pen. He hated being in the executive conference room. Nothing good usually came of it. Sighing, he looked at his phone. *Meeting should have started six minutes ago*, he thought. *I've got stuff to do!* Being the Director of IT for a global organization meant there was no shortage of work—fires to fight, initiatives to plan, and technologies to deploy.

Over the past few months, though, he had largely been focused on remote file access. More employees were either working in the field or from home, and needed access to files residing behind the firewall.

After a lot of research and phone calls, Jim had landed on a great enterprise level cutting-edge cloud solution. It ticked off most of the boxes for him—easy to provision new accounts, file access controls, collaborative tools across devices, and global availability. Which is why he was uncomfortable with the meeting his boss, Peter, had set up at the request of the company's Chief Privacy Officer and Corporate Counsel, Larry, to discuss remote file access.

What do they need to talk about? He wondered. *I solved this problem already!* Jim was about to check his phone again when the glass door swung open and Peter and Larry walked in.

"Do I need a lawyer?" Jim asked. Peter and Larry chuckled.

"Okay, Jim," Peter said, taking a seat next to him. Thankfully, everyone came down to his end of the table. "All joking aside, we need to address this public cloud problem. I know that you implemented a great new enterprise-grade cloud solution, but Larry brought up a very serious concern and I thought it best that you hear it from him directly."

"So, Jim, you are aware of the need to keep strict control over our data, correct?"

"So why are we here?" Jim asked, puzzled. "Tell him about the CLOUD Act," Peter

Larry asked.

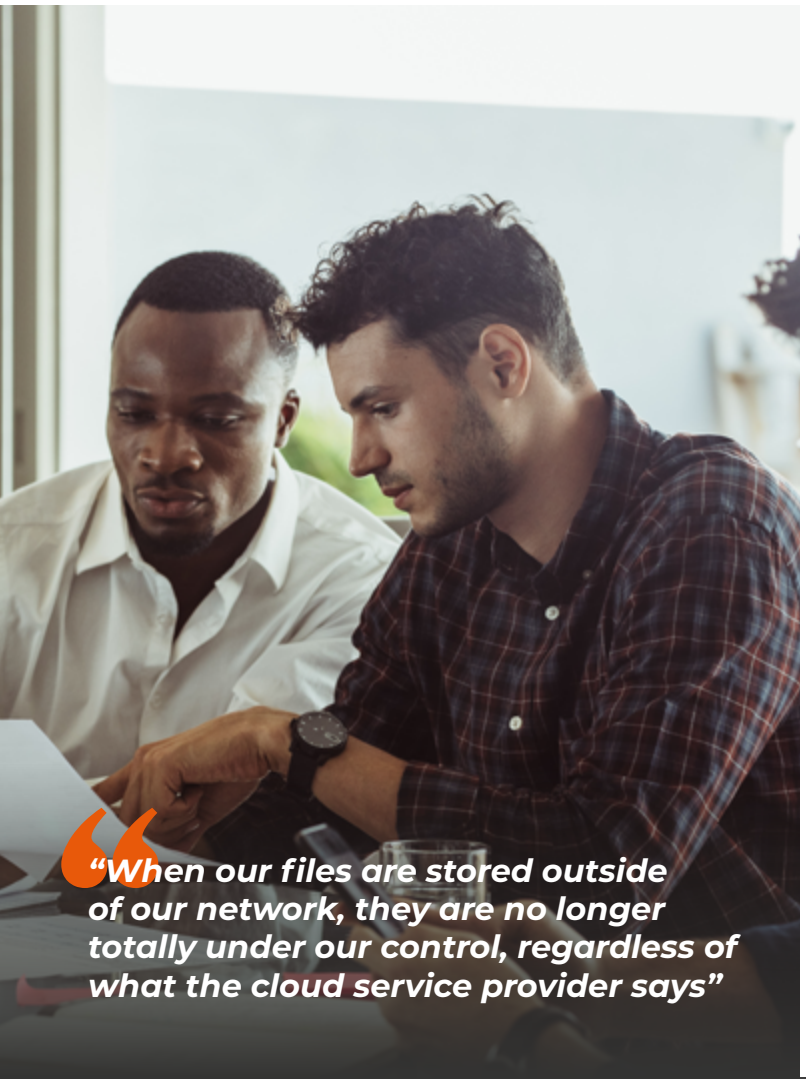
“Absolutely,” Jim said. “I understand the regulations governing data security in our industry. That’s why I went with my choice. It has lots of access control features.”

“Good,” Larry said. “So, let me explain my concern.”

He pulled some papers from a manila folder and slid them across to Jim who glanced at them.

“One of the main reasons we need to keep strict control over our files is to protect the privacy of our client and company confidential information,” Larry said.

“Right,” Jim said, nodding. “That’s why I made my choice. Our cloud service provider will ensure data residency so that we are in compliance with privacy regulations such as HIPAA and GDPR.”



“That’s great,” Larry said, “I’m glad you made privacy part of your decision making and selection process from the get-go.”

“So why are we here?” Jim asked, puzzled.

“Tell him about the CLOUD Act,” Peter said.

Jim looked up from the papers Larry had passed to him.

“I think we all know that 21st-century organized crime isn’t limited to geographic boundaries. In fact, sometimes they use those boundaries to hide and cover their tracks which has been problematic for law enforcement. To access information stored on servers in other countries, law enforcement agents have had to go through a long, cumbersome process to request access through international treaties.”

“Yes….so?” Jim asked. “Where is this going?”

"To enable law enforcement to pursue criminals more easily across international borders, governments have passed, and are in the process of passing, new legislation and agreements such as the CLOUD act and the E-Evidence Directive in the EU that allow them to more easily access files stored in cloud servers outside their geographic boundaries," Larry said. "Under certain circumstances, foreign governments can get access to our confidential files without going through the treaty process, without making a request to our local government and without out knowledge."

"In effect, data residency is no longer a guarantee of privacy," Peter added.

"Wow," Jim said. "I had no idea. So, basically, if this happened to us..."

"We would never know our files had been accessed," Larry continued. "Data exfiltration is now a real threat to the privacy and protection of our confidential information."

"But we don't have anything to hide, right?" Jim asked.

"Correct, but that's not the point. We are a multi-national company with employees and customers around the globe. Our executive team is very concerned that sensitive overseas customer data, regardless of where it's stored, could now potentially be legally sequestered and circumvent local privacy regulations. This ultimately puts our company at risk. Data residency no longer guarantees privacy. Data sovereignty is what matters now. Everyone is extending their jurisdiction over the cloud."

> ***Data residency no longer guarantees privacy. Data sovereignty is what matters now.***

"And, to top it all off, our privacy is further eroded because the cloud service provider themselves have always been able to access our stuff," Peter added.

"What about a private cloud?" Peter asked.

"It's expensive to maintain and I'd have to hire people with expertise to manage it and buy the servers and storage to run it,"

Jim leafed through the papers Larry had passed him again and looked at Peter. Then he looked at Larry.

“Okay, I get it. The solution I chose to enable remote access to files doesn’t ensure our data sovereignty.”

“Exactly!” Peter said. “Our data needs to remain on our property and under our control.”

“Listen, I’m not knocking your selection of our enterprise file sharing solution,” Larry said. “But the world is changing rapidly and the technology itself is what inherently creates these concerns. My issue is that it requires us to make compromises that could ultimately hurt the company, compromises that we shouldn’t have to make.”

“What about a private cloud?” Peter asked. “That would keep the files on our storage, rather than in the public cloud, and provide stricter security.”

Jim shook his head.

“Well, we could go that route, but it’s pretty complicated to setup correctly,” Jim said. “And, it’s expensive to maintain. I’d have to hire people with expertise to manage it and buy the servers and storage to run it.”

“Well, then, I think we need to revisit how we are allowing remote access and sharing,” Larry said. “I’ll be talking about this with the CEO in our next management meeting. I’d like to be able to tell him we’ve got an idea about how to address the issue.”

Peter looked at Jim and then back at Larry. “Got it. We’ll make it a priority.”

Jim felt like he had a bunch of long nights ahead of him.

Where Did Jim Go Wrong?

When Jim selected a remote access solution for the organization that employed enterprise-grade public cloud technologies, he made sure that it checked all the boxes:

- **Control**—the solution needed to include administrative features that enabled the company to completely control who accessed what files.
- **Security**—the solution needed to be highly secure, ensuring that all access was encrypted (via HTTPS) and employed two-factor authentication for login.
- **Collaboration**—the solution needed to include collaboration tools that enabled employees to better work together while remote.

In short, Jim selected a solution that both met employee needs to access important files while working remotely, and yet also ensured a level of IT control.

What Jim didn't know, though, was about the changing global political landscape and how new legislation, such as the CLOUD Act, could put both company confidential and customer sensitive data in potential jeopardy of exfiltration. He believed that the cloud provider he selected ensured their data sovereignty and jurisdiction. But, after his meeting with Larry, he knew that wasn't the case. And, he'd ruled out the idea of a private cloud or on-premise Enterprise File Storage and Sharing (EFSS) solution because of the complexity and cost required to maintain and configure all the components correctly. Now, though, the issue has executive visibility and Jim needs to find a solution that will allow employees to remotely work on files, share them, and collaborate while keeping data on company property, maintaining control, and protecting organizational data sovereignty and ensuring that private user data (like healthcare information) stays under the jurisdiction of local authorities.

Understanding the Cloud Act

The Clarifying Use of Overseas Data (CLOUD) Act was signed and enacted March 23rd, 2018. According to the Electronic Frontier Foundation[1], the bill creates an explicit provision for U.S. law enforcement (whether a local police department or federal agency) to access electronic files and communications stored in the cloud. In other words, 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. 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 exfiltated 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 would allow the Executive Branch to enter into "executive agreements" to allow qualified foreign governments to acquire data of their own citizens wherever located, with restrictions, without regard to U.S. law or the U.S. constitution.

In short, under certain circumstances, 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.

The Remote File Access, Sharing, and Collaboration Landscape

The remote file sharing and synchronization landscape is very mature. Organizations have been implementing technologies for decades that allow employees to access files while working away from the office. And many popular cloud services have implemented EFSS features that appeal to organizations looking for an easy-to-setup solution for remote file sharing and synchronization. The table below captures some of the technologies that have been used to provide this functionality.

Approach/Technology	Description	Issues
Virtual Private Network (VPN)	Allow employees to access secure network resources, including storage, remotely through an encrypted point-to-point connection	This really isn't a valid solution. Yes, it's possible that an employee could get access to network-attached drives via a VPN connection, but there's no opportunity for sharing, synchronization, or collaboration. This is just a dumb pipe.
Corporate Intranet (Microsoft SharePoint)	Allow employees to access sensitive data and other resources, including files, through a designated, private "web portal."	This is great for sharing when employees are connected to the network (i.e., via VPN) and can work in conjunction with files stored in Microsoft OneDrive for Business, for example. But, again, it's just a subset of files. If files aren't copied into a SharePoint page or OneDrive, they aren't available. Further, remote access can be difficult and sharing with external parties complicated.
Public Cloud (DropBox, Google Drive, Microsoft OneDrive)	Enable employees to remotely access, share, and collaborate on files by storing them on the servers of the cloud provider, outside the corporate network, accessible through web browser, desktop, or mobile application.	IT has no visibility or control over files stored in the cloud. Cloud addresses only a subset of corporate information and has issues of data residency, legal jurisdiction, third-party access, and secret access by law enforcement. It increases the organization's attack surface and besides having to manage multiple images and versions of files, it inherently creates a more complicated storage structure which translates to a higher risk posture.
Enterprise File Sync and Share (EFSS) or Content Collaboration Platform	Essentially a public cloud that provides IT oversight.	All the problems of a public cloud solution except that IT oversight is enabled. These solutions are also expensive and complex to implement.
Private Cloud	Has the same functionality as EFSS, except that the server and storage is hosted on-premise and is under the control of IT.	Although a robust way to share files remotely, this solution can be expensive to install and maintain, often requiring new servers and storage to support, not to mention the manpower required to continually maintain, update, and ensure proper operation. And even after implemented, besides issues of version control, it covers only a subset of organizational data.

As explained in the opening story, Jim explored a number of solutions, eventually deciding that that an enterprise-grade public cloud service with remote file sharing and synchronization features, provided what he needed without the hassle of an on-premise solution.

The Cloud?

Of course, Jim isn't alone. Many organizations are gravitating to cloud solutions for remote access. Companies like Google, Dropbox, or Microsoft appeal to companies looking for functionality to enable file share and synchronization for a number of reasons:

- **Upfront Cost**—without software or hardware to install, there is no upfront cost and the entire solution is OPEX, rather than CAPEX. This is especially interesting to organizations faced with upgrading legacy network storage or requiring additional storage to support business growth.
- **Comprehensive administration**—there are numerous features that provide a clear way for an organization to control user access to files.
- **Ease of use**—many users are already familiar with how to use public cloud services for file sharing and synchronization.
- **Integration**—several of the larger public cloud providers integrate with common applications (like Microsoft Office) both on mobile and desktop devices which provides for greater flexibility with file collaboration.

But, the public cloud isn't a silver bullet. There are drawbacks to selecting this approach:

- **Complicated file management**—managing which files are copied to the cloud is a manual process and can be time-consuming and challenging as demand for access grows; individual locations on network drives must be copied separately to the cloud in order to enable synchronization.
- **Multi-tenancy**—many public cloud solutions are multi-tenant, meaning files are stored on shared servers with other organizations.
- **Partial coverage**—only a small portion of an organization's data can be stored in the cloud, meaning critical content that needs to be remotely accessed or shared often sits in-house and is inaccessible.
- **Outages**—whether it's due to large-scale DNS attacks or power outages, a problem with a cloud provider can make files inaccessible to remote users.

And now, "data exposure" can be added to the drawbacks, as data or files stored on third-party servers are now potentially under the jurisdiction of multiple nation states. Organizations that utilize public cloud services for remote file sharing and synchronization are completely exposed.

A Brief History of EFSS (also called Content Collaboration Platforms)

According to Wikipedia[2], the EFSS market emerged in 2010 with over 100 vendors from a variety of different technology backgrounds including traditional storage, managed file transfer, and enterprise content management. Many of the solutions that came to market were created in response to consumer file synchronization and sharing services (i.e., public cloud services) that did not have the security, integration, or other features required by enterprise customers. EFSS solutions are often characterized by having some or all the following features:

- Sync files stored in corporate storage to user desktops and devices
- Send links to large files with support for multiple file extensions and protocols
- Integration to existing business applications via APIs, plugins and mobile apps
- Built-in file creation, editing and previewing
- User access permissions to files and folders
- Protection of files stored and transferred by encryption, antivirus scanning, and DLP (data loss prevention)
- Publish links to files with the ability to set a login requirement to access data
- Authentication options for Active Directory, SAML, Azure Active Directory, etc.
- Schedule and automate file transfers from automated systems and repositories
- Audit and report file activities and system actions

IT is not happy with EFSS

Cloud sync & share always results in some form of compromise

Wilson Research Group did a survey of IT personnel who play a role in EFSS purchase decisions and are in companies of more than 1,000 people.

The massive movement to the cloud

49% of CIOs intend to purchase new or additional file sync-and-share services in the next 9 to 12 months.

of CIOs will deploy hybrid cloud on-premises.

of CIOs will deploy private cloud on-premises.

** Source: Best Storage Products of 2016*

Chief drivers of cloud storage

What are the most important factors driving your decision to deploy EFSS?*

- They want to buy a service that allows employees the ability to collaborate on files.
- They want to provide the ability to share files
- They want to provide remote access
- They want to provide mobile access

In conclusion, CIOs purchase EFSS for the functionality NOT the storage!

Generally speaking, no one buys EFSS services because they need more storage. They are purchasing the functionality, not the storage.

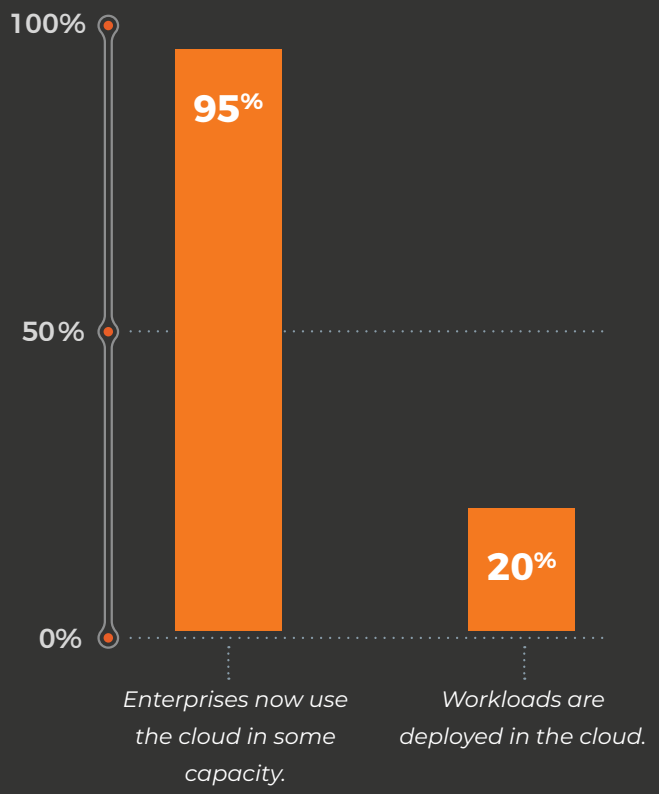
Going Private: Building Your Own Cloud

Sure, it's possible for an organization to deploy its own servers in data centers around the globe and install software, such as EFSS or private cloud platforms, to provide remote file sharing and synchronization in a completely controlled environment. But, as Jim found out, that solution is fraught with costs and difficulties:

- **Software**—on-premises EFSS and private cloud software can be costly both to license and maintain.
- **Configuration**—setting up a private cloud is more than just licensing software and buying servers. It requires network and software configurations to ensure security and file access that conform to an organization's GRC framework.
- **Maintenance**—private clouds require on-going maintenance including infrastructure (updating hard drives and storage devices) and software (both the cloud platform and file sharing service).

But, "data exposure" is contained. Organizations that keep their data on their servers ensure that no one else can ever access corporate files without authorization.

Even though cloud adoption is high, most workloads are on-premises



Managing the Tradeoffs

Unfortunately, none of the current remote file sharing and synchronization solutions adequately address Larry's primary concern—affordable and simple protection of data sovereignty. Ultimately, it's a tradeoff. An organization can go the easy route and subscribe to a public-cloud service, synchronize files with it, and start enabling their employees with remote access across devices. But, as illustrated in the opening story, the organization may put the privacy of that data at risk of potential exfiltration and undermine their data sovereignty. Or, an enterprise can go the hard route and setup a private cloud, virtual private cloud or a on-premise EFSS software, indicate which files to share from network storage, configure security and firewall access, and turn-on remote sharing.

Regardless of the technology, any remote file sharing and synchronization solution should address four critical areas:

- **Security/Privacy**—when company files are stored with cloud providers, they may not be safe from exfiltration …no matter where they are physically stored. This creates significant problems with protecting and safeguarding the privacy of sensitive customer data.
- **Compliance**—there are many national and foreign governmental regulations concerning how sensitive, personal customer data must be protected. This means that employees viewing documents in public, or data being transported across country borders, may be in violation of such privacy regulations such as GDPR.
- **Costs**—let's face it, to address all the security concerns, remote file sharing and synchronization solutions must be on-premises which keeps files on network storage and behind the firewall. But doing so can require additional capital investment in dedicated storage, additional servers, and, of course, the manpower to keep it all running. Some industry estimates peg these solutions at $120+ per user, per month.
- **Productivity**—the ultimate reason for enabling remote file access is to improve productivity when employees are away from their computers. Without access to files when they need them, whether that's waiting for a subway or working with a customer, an employee will have nothing but downtime. Sure, employees can request files via email, which is adequate to move documents around, but large attachments can easily choke the email service and poor connectivity can hamper downloads. And even with existing EFSS solutions, there's little opportunity for users to collaborate on documents without downloading and using third-party applications.

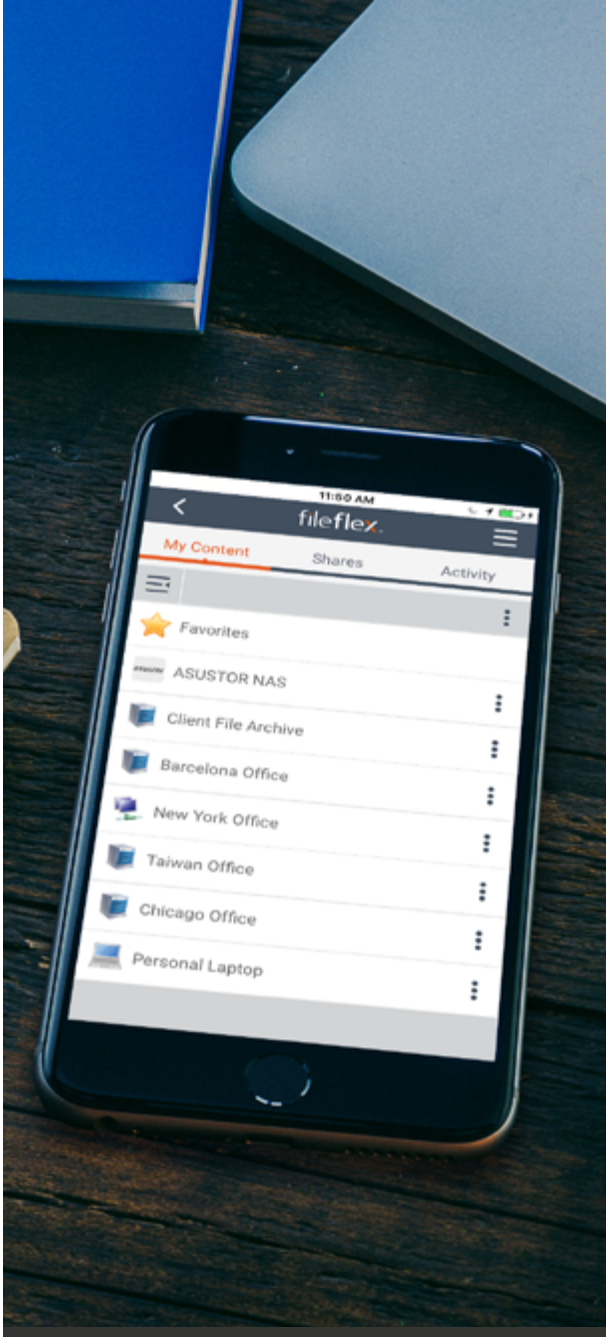
Yes, Jim dismissed on-premise EFSS as too costly, but if the technology meets Larry's privacy needs, he's going to have to move in that direction. Or, more importantly, he needs a solution that provides the ease and simplicity of the cloud with the protection of data sovereignty provided by on-premise software. Files need to remain on the corporate network. Access controls must be maintained. Security and compliance must be addressed, regardless of the cost. All while addressing a new priority....

Data Sovereignty: The New Priority

As organizations adopt public cloud technologies to enable remote file sharing and synchronization, they must prioritize data sovereignty. By storing files on third-party servers, they are granting potential access to governmental entities and undermining their own data sovereignty as the protections once afforded by data residency continue to erode. The result? Increasing the risk of unknown data exfiltration. Under the new legislation, nation states don't have to seek the permission or notify either local authorities or the organization itself to request file access from enterprise-grade public cloud servers.

> ***To protect the privacy of your company information, you need to keep your files on your own property.***

Is your organization willing to risk privacy and possible exfiltration of company and client confidential information? Are your customers? If the answer is "no," then cloud solutions shouldn't even be a consideration. Jim is probably already regretting his choice for remote access knowing what he does now. Frankly, to protect the privacy of your company information, you need to keep your files on your own property.



Is Your Remote File Access REALLY Secure?

Even if you are employing an EFSS solution, there's a good chance that file access is happening in the clear. And with users often employing publicly-available WiFi with their mobile phones (to save on data charges and improve connectivity), that means the available files through your EFSS or private cloud software are at risk too.

An on-premise EFSS solution was clearly the way to go, but the benefits of current offerings are outweighed by the complexity and cost of implementation. If Jim can't find an adequate, cost-effective solution, there's a distinct possibility his company may forget about enabling employees with remote file access all together which may, unfortunately, leave employees to their own devices (i.e., public cloud accounts) and take away all IT oversight. This would, of course, put the company at significant risk.

FileFlex Enterprise:

Using Edge Technology to Enable Remote Access, Sharing, and Collaboration

In their conversation, Jim, Peter, and Larry identified a fundamental issue—ensuring data sovereignty and protecting data jurisdiction—that any remote file sharing and synchronization solution must address. Jim and Peter, in charge of the company's IT resources, must also balance that need with other requirements such as compliance, cost/complexity, and productivity tools. FileFlex Enterprise addresses each of those concerns in an end-to-end encrypted environment:

- **Security/Privacy**—with a permissions-based approach, access to files can be granted in real-time from any network storage attached to the FileFlex Enterprise platform. Attaching a new storage location (anything connected to the network) is handled effortlessly and easily through the administrative interface. And, because files are only stored on corporate network assets there is no worry about data exfiltration through the new legislation. Sovereignty and jurisdiction are maintained!
- **Compliance**—by employing a "virtual private cloud" (that only exists within the scope of the FileFlex Enterprise platform), files are physically stored where they need to be (i.e., in specific geographic locations) to meet regulatory requirements. There is no need to copy files to different locations for sharing.
- **Cost**—FileFlex Enterprise leverages existing network storage (i.e., servers, NAS, SAN, etc.) rather than requiring shared files to be copied to cloud locations. It also doesn't require any new servers to be installed or additional private-cloud infrastructure.
- **Productivity**—baked into the FileFlex Enterprise platform is a suite of collaboration features (including versioning control) that enables multiple users to easily modify some document types.

Never Underestimate the Need for Security

As more employees access more files remotely, the threat surface increases exponentially.

Although technologies like VPNs and HTTPS can ultimately help secure transactions between employees and EFSS software, there's still the opportunity for problems to occur. What if the VPN isn't configured correctly and the employee accesses files through an alternate means... via public Wi-Fi? What if the HTTPS certificate expires or isn't configured correctly enabling files to be accessed "in the clear?" FileFlex Enterprise, in conjunction with Intel vPro technology, solves this problem by providing silicon hardened encrypted hybrid point-to-point communication with no duplication, no third parties, and all files are kept in source locations behind the firewall.

This brings superior privacy and security, along with a significantly reduced threat surface, together with simplified storage structure and governance, risk management and compliance (GRC) that is under the user's control. And when you add sharing that is restricted to permitted contacts only, two-factor authentication, device authentication, real-time activity logging, single sign-on, active directory integration and operation and incident management, you have a solution that offers confidentiality, integrity and availability capabilities (CIA) with minimal impact on existing processes and infrastructure.

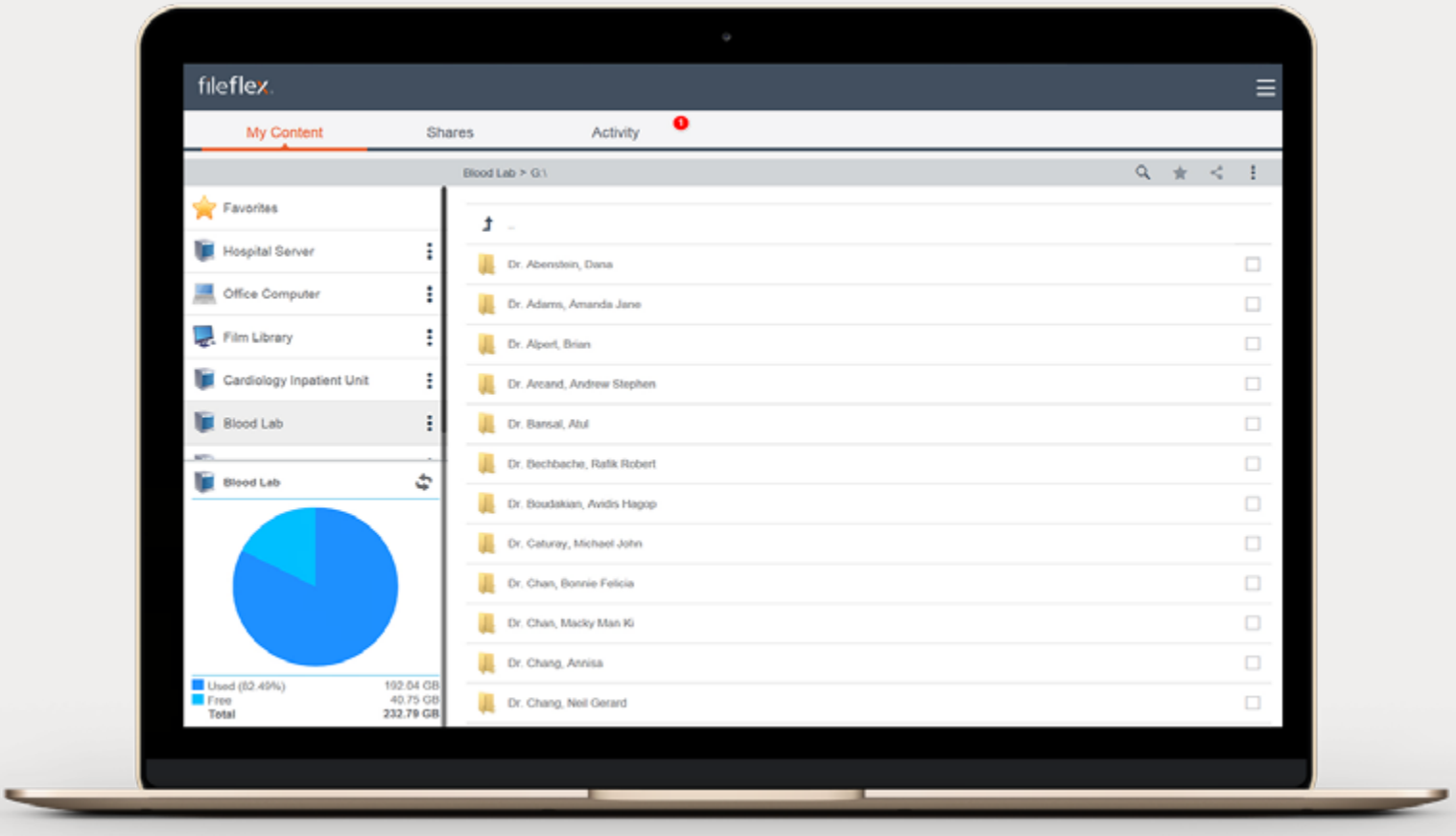
With a simple network software installation, IT can fully enable the entire organization with remote file access while maintaining complete access control over shared files.

Under the Hood with FileFlex Enterprise

What makes FileFlex Enterprise different than current EFSS solutions? FileFlex is a powerful edge-service that works with browser- or application-based file access from both desktop PCs and mobile devices.

FileFlex Enterprise is exactly what Jim, Peter, and Larry need to collectively address the problem of potential governmental access to files stored in public cloud services. Not only is it simple to install and maintain, it doesn't require any additional infrastructure, making it a cost-effective alternative to EFSS solutions. And because it enables sharing of files from their existing network storage locations, there's no need to copy files to dedicated storage or move them to a cloud service, ensuring that they remain private, secure, and under corporate domain. Finally, with granular access controls (based on permissions that can be enabled in real-time), IT stays in complete control of who has access and where files can be shared.

So, how does FileFlex Enterprise address all the issues?



Security/Privacy

If the EFF's interpretation of the CLOUD Act is correct, Larry is rightfully concerned about potential data exfiltration by foreign powers. But, with FileFlex Enterprise, files remain secured behind the corporate firewall, on corporate storage assets, protected by whatever security solutions have been implemented. Through an intuitive administrative interface, enterprise IT resources can granularly protect the right to access files through a permission-based system which can be changed in real-time. There is no chance any third-party can gain access to files without the organization's knowledge.

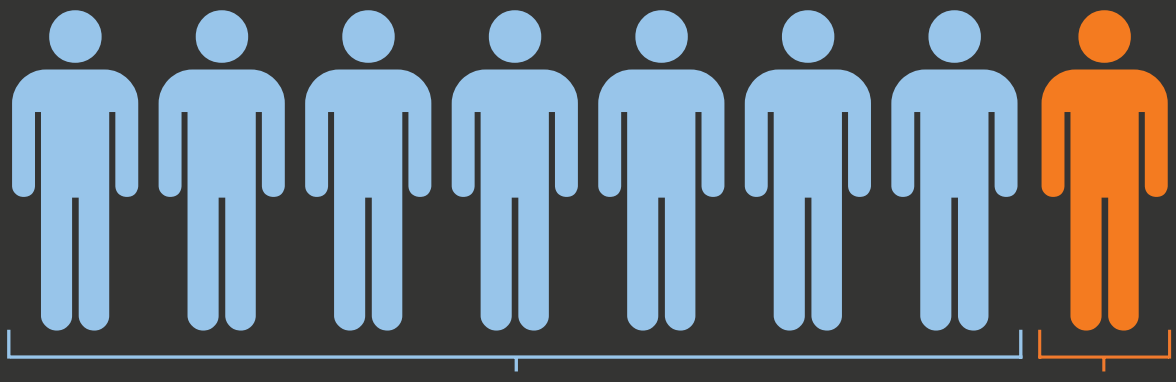
Peter and Jim will be satisfied that they can protect access to sensitive information.

Compliance

By keeping files in their original location—behind the firewall, in specific geographic regions, and access controlled—a company can rest assured that they are following specific governmental privacy regulations like HIPAA and GDPR. When files are placed in the cloud, for example, they may be synchronized by the SaaS operator across multiple data centers around the world and shared by users through links and other means. FileFlex Enterprise includes powerful administrative controls to ensure that files exist where they should and are only shared with the people, and in the regions, where it's legally appropriate.

Larry can rest assured that the company is complying with all regulatory requirements.

CIOs prefer on-site solutions



RATIO:

IT personnel who support the logic of owning and controlling a file, sync and share service on-site

IT personnel who prefer off-site EFSS

Cost

With FileFlex Enterprise, no employee needs a public cloud account to access their files remotely. What's more, by utilizing all the storage resources in the corporate network, the company can take full advantage of their existing capital investments. Finally, FileFlex Enterprise doesn't require any additional infrastructure (i.e., Servers, VPN, etc.) and can be maintained easily by a single administrator.

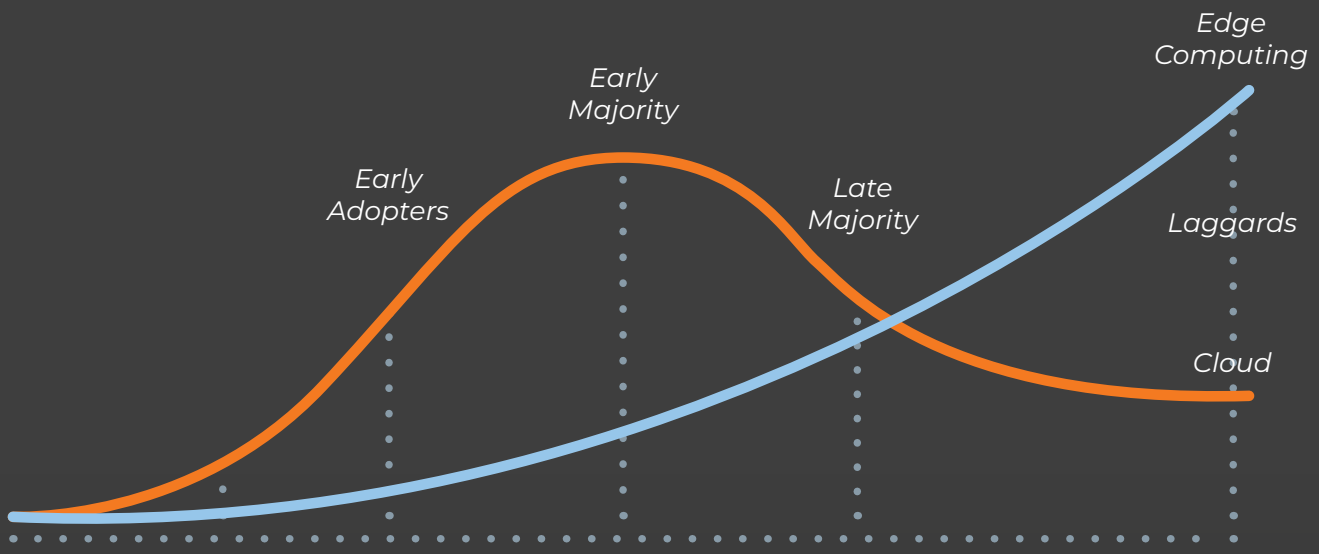
Jim can rest assured that this solution for remote file sharing and synchronization doesn't have anywhere near the complexity or costs associated with traditional EFSS software.

Productivity

Accessing files is one aspect of productivity, but being able to collaborate with fellow employees means remote users in the field can get work done whether on a laptop, tablet, or smartphone . Collaboration uses existing third-party software such as Microsoft Office 365 (Microsoft Word, PowerPoint and Excel), Google Docs, AutoCAD, Illustrator, PhotoShop, and InDesign.

The company's executive team will be happy to know that their remote employees can work together while out of the office.

Cloudless solutions represent next wave of



- Arguably cloud adoption may have reached the early majority or peak of the bell curve – meaning new, better solutions, like Edge Computing are emerging.
- Edge Computing to surpass EFSS by 2020 to be a $6B segment with 40% CAGR (Gartner) vs $3.5B and 25.7% CAGR for EFSS (Markets and Markets)

It's Friday...

"Good to see you again guys," Larry said as Jim and Peter walked into the executive conference room again. "So, what do you have for me?" Jim looked at Peter.

"This is all you, Jim," Peter said. "You found the solution."

Jim smiled and opened his laptop. He plugged it into the projector and brought up the FileFlex website. "It's called FileFlex Enterprise," he said, "and it might be the perfect solution."

Larry raised an eyebrow as he looked at the screen.

"It provides the functionality of the cloud to all of our existing corporate storage located in every facility we operate worldwide. All our files stay on our servers."

"So, no need to copy files into a cloud," Peter chimed in.

"Exactly," Jim continued. "And, it's super simple to install and maintain."

"Wow," said Larry as he looked away from the screen to Jim. "Okay, is it really new? Unproven? Untested?"

"No," Peter chimed in. "Although they are a young company, they've spent years developing the technology and even announced a huge partnership with Intel which provides silicon-to-silicon access secured by Intel SGX platform-based hardening to protect against snooping and intercept, even on systems that are compromised by malware."

"I'm sold," Larry said. "How long will it take to get up and running?"

"Well," Jim said as he opened FileFlex, "that's the really good part. It's already installed on our network. Here, let me show it to you..."

It May Not Ever Happen, But If It Does...

It's quite possible that the EFF and other interpretations of what might happen under the CLOUD Act may never befall your organization. But, if you are using cloud services, and it does happen, the ramifications to your business may be significant. They may undermine customer trust. They may damage your brand. They may even impact revenue as customers look for a partner that is more secure. Now is your opportunity to protect your data. You know your increasingly mobile employee base needs remote file access. You just need to ensure such access is secured and that your files are safe from possible exfiltration while also providing productivity, compliance, and other features. The FileFlex Enterprise platform is the evolution of EFSS technology, enabling organizations of any size the opportunity to enjoy remote file sharing with the peace-of-mind that it is always in control of its data and files.

References

1. https://www.eff.org/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection-race-bottom
2. https://en.wikipedia.org/wiki/Enterprise_file_synchronization_and_sharing

Credits

Author:
Jason Thibeault
https://www.linkedin.com/in/thejasonthibeault/

Sponsor:
Qnext Corp.