BEYOND EFSS

Confronting security issues inherent in Enterprise File Sync and Share

By George Crump and W. Curtis Preston

Storage Switzerland, LLC

SUMMARY

In order to address the security issues of cloud computing, the cloud industry sector responded with the Enterprise File Sync and Share (EFSS) solution. This is essentially a cloud that provides IT oversight and addresses the issues of employees using public clouds. But you may be surprised at the security issues that you can still find inherent with all EFSS solutions. Issues that just don't get talked about much.

This e-Book written by industry leading experts at Storage Switzerland explores the issues EFSS vendors don't give much air time. It will help you to understand the security implications of EFSS before embarking on any long, complicated and expensive implementation.

INTRODUCTION

The workplace acceptance of the mobile phone and tablet have brought disruptive change to the way modern workers work. As people travel with their new devices, they expect and demand that all of their information travel with them. They now expect that any file they need is available to them on any device they are working on from anywhere. The legacy device-centric data paradigm has been replaced by data continuity.

To be even more productive and remotely work on multiple devices, workers have turned to the cloud -inadvertently putting the organization at risk. Additionally, when employees who have cloud accounts leave the company they – and any others who have the links – can still access the business content stored there, posing an indefinite legal and security risk to the company. With consumer grade file sync solutions, monitoring is virtually impossible. There is no audit trail and the enterprise faces compliance issues. When corporate data is not contained on your company-owned IT infrastructure, it is impossible to control or even know who has accessed it, who has copies and who it has been shared with.

In order to address the security issues of cloud computing, the industry response was Enterprise File Sync and Share (EFSS) solution. This is essentially a cloud that

provides IT oversight and addresses the issues of employees using public clouds. But you may be surprised at the security issues that you can find inherent with all EFSS solutions. Issues that just don't get talked about enough.

When organizations store their files with an EFSS vendor, they are storing them on a server that is owned, operated and located on the property of another organization. But, there are issues inherent with storing your organization's files on someone else's computers. First, all files stored with EFSS are duplications. This increases your threat surface, complicates your storage infrastructure and at best shares governance, risk management and compliance (GRC) with someone else. This translates into an increased risk posture. Second, since your files are no longer on your own property, behind your own firewall, you add to that issues of data residency, jurisdiction, third-party inspection and secret access by law enforcement.

Finally, EFSS storage is an expensive subset of your organization's storage, meaning critical information may not be available when needed.

This paper explores these and other issues that EFSS vendors don't talk about. But they are issues nonetheless. This e-book will make you aware of some of the problems you need to overcome before embarking on any long, complicated and expensive implementation of EFSS – hybrid or other.

Finally it presents FileFlex – a very secure, software-only, enterprise-grade solution where there is no cloud required. It adds all the functions, features and benefits of EFSS to every file on your storage infrastructure , but keeps all your files on your own storage, behind your own firewall, under your own Government, Risk Management and Compliance (GRC), simply, at a fraction of the cost, turning it all effectively into a virtual private cloud.

CHAPTER 1:

Enterprise File Sync and Share is Broken... just look at these facts

By George Crump, Lead Analyst

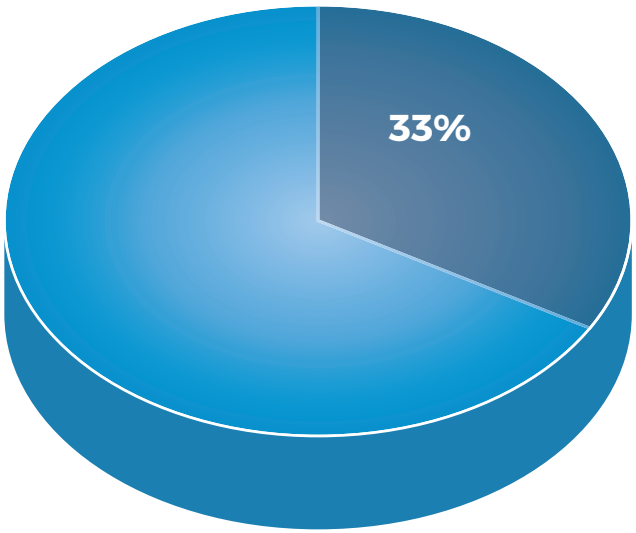
It seems like every CIO has enterprise file sync and share (EFSS) on their project whiteboard. The problem is that it is stuck there and the alternative, users doing their own thing, seems sort of acceptable. Most EFSS solutions are too disruptive and require a big commitment to the cloud which many organizations are still uncomfortable with. Combine these issues with an apparent lack of urgency and it's no wonder EFFS never moves from the to do list to the done list.

What is Enterprise File Sync and Share?

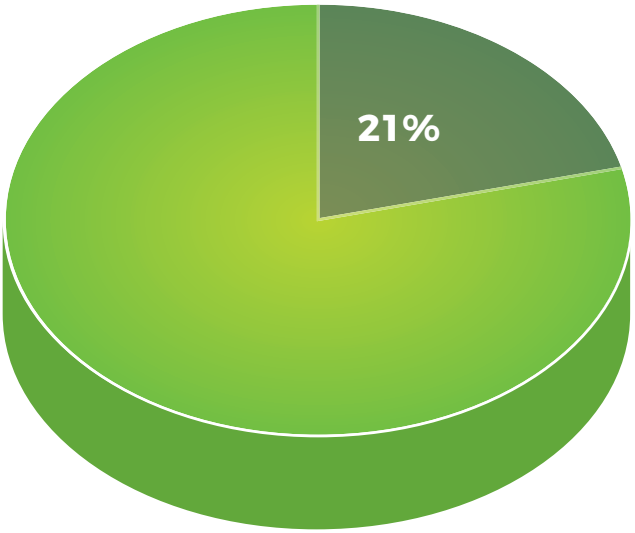
File sync and share is a service where data is stored or synced to a server that can be accessed over the Internet. It has been made popular by companies like DropBox, Box, Google, OneDrive and Apple who generate massive amounts of revenue through its sales. Originally the technology started as a means to make sure that all of a user's devices had the same data on it. Sharing was added to these services later, enabling users to provide access to their files to their colleagues instead of having to email files back and forth.

The important thing to realize with file sync and share services like Dropbox and Google Drive is that the server is not owned by you, is not under that user's control and certainly not the organizations. It is owned and under the control of a third party (ie. Dropbox or Google).

EFSS is the corporate implementation of the initial consumer FSS service. It generally means the organization will provide a similar FSS capability as the consumer solutions but do so with-IT oversight. Typical features control what data users can share, who they can share it with, how long the user can share specific files and provide the ability to revoke access to the files if the employee leaves the company or one of their devices gets stolen. It is important to note here that if the EFSS service is not hosted on-premise the organization is putting corporate data on a server that is owned and under the control of the EFSS provider.



Implementing New EFSS



Replacing Existing EFSS

According to Wilson Research Group, 33% of IT decision makers in companies of more than 1000 employees plan to implement a new EFSS solution in the next year and 21% plan to replace their existing EFSS solution. IT prefers on-premise solutions to off-site EFSS by a ratio of 7:1.

IT Must Provide EFSS

Workers are more mobile today and use multiple devices. They start a task on one device, but work and finish tasks over multiple devices and often involve multiple people. According to a study commissioned by Facebook, 40% of all online adults start an activity on one device and finish it on another.[1] Today we expect to access our files from any of our devices no matter where we are. Data is not centric to my device, there needs to be data continuity between all my devices.

The same is true for working alone vs working in collaboration with others. Data is not centric to a single person, there needs to be continuity with others. File sync and share services are simply the tools that workers turn to for data continuity, device continuity and user continuity. They need them so they can be more productive. According to a study commissioned by Intel, when employees have access to the content they need on their devices of choice, productivity increases.

In a study from 2010 to 2012, Intel estimated that they gained more than 7 million hours of productivity because of their ability to use BYO devices that have access to the content they need.[2]

If an organization does not provide users with EFSS, they are forced to get it on their own via a free or inexpensive consumer-grade public FSS solution like Google Drive. When employees open accounts with consumer file sync solutions, they introduce security, and regulatory and content leakage risks to their companies. In their efforts to improve productivity and collaboration these employees inadvertently put the enterprise at risk. Additionally, when employees who have

[1] Multi-Device Usage Study by GfK Nov-Dec 2013. Study commissioned by Facebook. Survey of 2,018 UK online adults and 2,004 US online adults

[2] 2012-2013 Intel IT Performance Report, Deploying an Enterprise-Ready Content Sync-and-Share Solution

such accounts leave the company they — and any others who have the links — can still access the business content stored there, posing an indefinite legal and security risk to the company. Even when employees simply abandon their accounts, the company has no way to remove the business content. With consumer grade file sync solutions, monitoring is virtually impossible, there is no audit trail and the corporation faces compliance issues, either self-imposed or regulatory.

When corporate data is on consumer FSS, it is impossible to control or even know who has accessed it, who has copies and who it has been shared with. The moment that duplication to an FSS service occurs there is no audit trail of where the data went, violating all the security safeguards created by Active Directory. Ignoring file sync and share puts the organization at massive risk and makes it more vulnerable.

EFSS is Compelling but it does have ongoing problems

The case for EFSS is compelling – but there are some real problems that, based on the current technology and legislation, will be hard to overcome. EFSS should provide the same capabilities as FSS but keep organizational data more secure and reduce costs. For the most part, many EFSS solutions do an admirable job of addressing issues of IT oversight and control.

EFSS, though, introduces its own challenges. First, most solutions introduce data duplication. Files are being copied or synced from the source computer to the specialized server that allows internet access.

Duplication of data introduces a duplication of security concerns, administration, complexity, resources and cost. Further, when data is duplicated to the server of the EFSS provider it also creates issues of content ownership, third party inspection, jurisdiction, data residency, and legalized secret access by law enforcement. For example, when Amazon recently acquired Whole Foods and became a brick and mortar merchant, Walmart quickly prohibited its vendors from using Amazon cloud services due to their concerns about the legal third party access rights that Amazon has to examine the confidential information about Walmart that its vendors may have stored on Amazon's servers.

Second, because most EFSS services are a duplication of data to a specialized server, they, by definition, can only address a subset of an organization's files. This means that often critical content that needs to be remotely accessed is inaccessible.

Another issue is availability and breaches. For example, all the major consumer solutions suffered an outage in the last year. In fact, the number of and frequency of outages appears to be on the rise.

Moving to either an on-premise or public-based cloud also creates an economic challenge. Remember most of this data is not net new. It exists already, and it is stored on something. In other words, the organization has already invested in storage and probably has plenty of available capacity to continue to store new data. This means that unless they are ready to refresh storage, the organization must

re-buy something it already has just to get file sync and share! This is an expensive option. Even if the organization rationalizes the purchase of additional storage, then the data needs to move either to the cloud or to another storage system on-premises. Data Migration is a constant source of heartburn for IT professionals. The process is complicated, time consuming and wrought with potential for error. Introducing another migration project when it is not even needed will not be well received by IT administrators.

Another shortcoming is that most of these solutions don't acknowledge that most organizations started down the consumer file sync and share path long before they realized the risk and vulnerabilities those solutions introduce. In other words, there is data in those services that needs to be accessed, controlled and eventually consolidated.

When you add up issues associated with EFSS you realize why it is a compromise that IT will switch from if presented a viable alternative. According to Wilson Research Group, 33% of IT decision makers in companies of more than 1000 employees plan to implement a new EFSS solution in the next year and 21% plan to replace their existing EFSS solution. IT prefers on-premise solutions to off-site EFSS by a ratio of 7:1.[3]

Storage Swiss Take: Next Generation EFSS

What's needed is a better way to implement EFSS. Obviously, the next generation of EFSS solutions need to build on what current solutions do well; provide oversight and control. Beyond that though a next generation solution needs to apply to all storage, not just a subset and it needs to address issues of duplication, security, ownership, third-party access and inspection, jurisdiction, data residency, legalized secret access by law enforcement, cost, data migration and IT administrative burden. It should support, but not require, a cloud-based component, and ideally provide the connectivity to existing services. It should also be able to add capabilities to existing storage and not require organizations to re-buy storage or require IT to perform a lengthy migration job.

Organizations need to provide employees with EFSS. The modern worker is too mobile (BYOD is here to stay) and organizations are too interconnected to operate without it. Monitoring and control are table stakes. To accelerate adoption, organizations need a next generation EFSS solution that addresses the shortcomings and compromises of today's solutions and operates in place, behind the firewall, removing concerns over the cloud, security, data movement and data residency while lowering costs.

[3] Computer Technology Review "New Research Sheds Light on How to Effectively Manage your File, Sync and Share (FSS) Strategy"

CHAPTER 2:

Why the Cloud is a Problem for Enterprise File Sync and Share

By W. Curtis Preston, Senior Analyst

Some see the reliance on the public cloud as the Achilles' heel of enterprise file sync and share (EFSS). While EFSS products are more robust than their consumer-grade counterparts, their use of the cloud does add a number of concerns that IT should address. Some of those concerns include security, data management and vendor lock-in.

The Cloud Security Problem

The biggest concern that most people are worried about when they talk about the public cloud is security. Not all EFSS products are created the same when it comes to security and that is the real problem. Some public cloud vendors adopt very strong security practices that are equivalent to those found in corporate IT departments; some do not. This is why a recent Wilson Research Group survey found IT personnel considering an EFSS preferred owning and controlling their own files to surrendering them to a cloud service, by a ratio of 7:1.

A lot of cloud security concerns center around how an individual user is authenticated. Many systems use simple password authentication, and some store and transmit the password in clear text. (If the app is able to send you your current password if you forget it, then they are storing it in plain text.) Other companies store the password encrypted, but it is not "salted" with random data in order to make it significantly harder to decrypt using brute force techniques.

Even if a cloud product supports two-factor authentication, it might be easy to get around the second factor. The most common second factor is an SMS message, which is better than nothing, but it's easily intercepted and faked. A recent Wired article discussed how hackers using social engineering attacks can easily hijack an SMS message, and more sophisticated attacks can simply do it grab it in transit. Another issue with two-factor authentication is many systems only use the second system if a boundary is crossed, such as

logging in on a new system. If someone gains access to an already connected system, they will not trigger a two-factor request and can do significant damage.

The biggest risk with only requiring the second factor on new devices are devices that have already been authenticated to a given sync directory, but have now been lost or stolen become a threat. Sophisticated corporate espionage attackers know what kind of EFSS the organization is using, and know that all they have to do is steal the right laptop to access the organization's data. IT should carefully inspect EFSS solutions to see how easy it is to revoke a device's access to data within the EFSS system or architecture.

The Data Residency Problem

Another security-related concern is data residency. In order to safeguard the privacy of its citizens, the European Court of Justice struck down the 15-year-old "safe harbor" agreement with the U.S. This forces Europeans to store their files on cloud servers located in Europe, under European jurisdiction and European law. In fact more recent laws require certain data to stay behind your firewall (e.g. banking, finance, legal, health, etc.)

Many companies and countries have policies or laws that dictate data of a certain type remain within the borders of a given country or region. The U.S., Australia, Hong Kong, Canada, Germany, Italy, Luxembourg, Mexico, the Netherlands, Singapore, Switzerland and the U.K. regulate data residency for some types of information such as government files and healthcare records. In addition, many professional associations such as law, accounting, finance, mortgage brokers and banking have professional, and in some cases government standards for their members that include data residency requirements to govern the use of cloud service providers and to keep information within a defined geographic jurisdiction. The reason is simple. They do not want personal and confidential files to come under the jurisdiction of a foreign power.

Cloud storage holds a treasure trove of information from many users and organizations and is a high value target for both hackers and national security agencies. According to a study from Skyhigh of 18 million users,[1] 21% of files uploaded to cloud providers contain confidential information such as personally identifiable information (PII), protected health information (PHI), payment card data, or intellectual property. Knowingly or not, 34% of users have uploaded sensitive data to the cloud.

Unfortunately, many public cloud providers are leveraging data centers all over the world for cost and latency reasons. Data residency concerns can become quite problematic. True, organizations can deal with data residency contractually, but it also must be policed on a continuing basis to make sure the data is never stored outside the boundaries specified by a given customer – and ensuring that data is meeting this standard can actually be quite difficult from a customer viewpoint. All the confusion of exactly where data is at any

[1] Skyhigh: "LastPass Breach By The Numbers: 91% of Enterprises Exposed".

given moment in time is probably another reason why administrators prefer owning personal data to storing it in the cloud.

Legal Jurisdiction Issues

Even if you comply with data residency, you may still have cloud security issues when protecting your confidential files from foreign jurisdictions. If the cloud provider is a U.S. company, it can be served with a U.S. search warrant for content it has in its possession regardless of where that content is located. This principle applies not just to the U.S, but to all nations and all jurisdictions. The lesson is this - when you store data in the cloud, even if the files are stored on servers located in your own country, they may still be under the jurisdiction of a foreign power.

Secret Access by Law Enforcement

What about law enforcement trying to access your data? With remote 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.

GDPR and HIPAA

Because of the above issues created by the use of cloud and EFSS providers, in order to protect their citizens, governments are instituting sweeping data residency and privacy laws such as the General Data Protection and Regulation (GDPR) of the EU and the Health Insurance Portability and Accountability Act (HIPAA) in the US.

The Cloud Transfer Problem

Another challenge with the public cloud is that it is on the other side of an Internet connection. While large transfers tend to slow down once a company is completely online with an EFSS system, problems arise when the company adds new devices to the network, or existing devices must be resynced. A significant amount of data will need to be synced to the cloud or from the cloud in order to bring that device into the fold, and that amount of traffic can create quite a load on the Internet connection.

Another transfer concern about the public cloud is once all of the organization's data is synced up to the cloud – and that may take a significant amount of time – changing cloud providers can become quite problematic. If the organization wants to change cloud providers, an entire re-sync of all content is required. But the path from one cloud vendor to another cloud vendor can actually be quite difficult, because vendors simply don't want to make it easy. In most cases, IT has to download all the data back into the data center and then send it back to the new cloud provider. The result? Organizations can get locked in to cloud providers.

The Attack Surface

A final concern of having sensitive data stored in the cloud is it gives hackers another place from which to grab sensitive data. EFSS providers create multiple copies stored in multiple locations of the information they hold.

It goes without saying, that if the available attack surface is minimized, the ability for an adversary to successfully breach through an organization's defenses becomes more difficult. At the same time, an organization can manage a smaller environment better than a large and complex one. Overall, this translates to a lower risk posture.

The Chain of Custody Problem

Finally, what about chain of custody questions? Consider, for example, the Target hack of customer data that was initiated by someone who stole credentials from one of its vendors. EFSS data should be tracked and audit logs should be available centrally for forensic examination at a later date. Unfortunately, many EFSS vendors do not provide any of these tracking or auditing features.

Governance, Risk Management and Compliance

Finally, with the growing pressure to empower employees, business associates, and customers with the latest EFSS technologies, governance, risk management and compliance (GRC) issues around the information stored on their servers has become a factor in your organization's security strategy. However, if using EFSS, your GRC management could be undermined, compromised or nullified and is at best shared with a third party. Use EFSS and your 'latest technologies' can quickly become a compliance headache.

Storage Swiss Take

Some file sync and share products are starting to examine this reliance on public cloud. If they can offer you the advantages of EFSS without the disadvantages of the public cloud, they might offer a real alternative to the status quo. Leveraging devices (e.g. SAN, NAS, desktops, laptops) that are already in place and behind the organization's firewall, versus cloud or EFSS solutions solves many of the problems mentioned above, especially those revolving around the security, as well as the performance and bandwidth issues of synchronizing large amounts of data to some third parties.

CHAPTER 3:

File Sync and Share Often Creates a Data De-duplication Problem?

by W. Curtis Preston, Senior Analyst

File sync and share is here to stay, and enterprise file sync and share (EFSS) is how most enterprises add this functionality to their environment. The question we are asking is whether the addition of this new service adds additional problems. For example, many EFSS solutions require data to be synced to another destination (either the cloud or a specialized appliance), creating yet another copy of data that IT needs to manage. Is there another way to add the same service without adding these problems?

Duplicate Copies Are Already A Problem

With unstructured data, we tend to create duplicates when we share data with other users, because we tend to send them via email, Skype, Slack, or other similar mechanisms that by their very nature create multiple duplicates of each file. Every one of these duplicates increases storage costs and complexity, while also giving hackers another place to attack the files. Duplicates caused by sharing files is one of the problems most EFSS systems are trying to solve. The fact is that today most systems require users to actually make duplicates in order to use the system. Duplication increases the threat surface of the organization and complicates the storage environment. This is creating a significant risk management and security problem for many companies.

EFSS Compounds the Duplication Problem and is Costly

For an EFSS system, even the hybrid versions, to begin sharing files each user needs to synchronize their entire directory to a secondary source. Once that synchronization is complete, the files must be synchronized to each user that will access them to a special directory, including the originating user. The first copy data challenge with EFSS systems is before a customer even begins sharing files, they must first create several duplicates of each file. In addition, EFSS providers have multiple

redundant servers at different geographies. Each server will also have a near-line backup and perhaps an off-site backup. EFSS systems are therefore adding to the duplication problem, not solving it. Again, this increases storage costs to the organization and security risks to the data.

The EFSS Transfer Problem

The next challenge with this model is the physics of getting everyone's user data to each location. If the central location is a cloud storage system, a significant amount of data will need to be transferred from the current location of the data to the cloud location over the Internet. As mentioned previously, that data will then need to be downloaded, also over the Internet, to each user that will share the data. The amount of bandwidth required for such transfers, and the impact on the environment during the transfer can be significant – that's expensive and not very productive.

Duplication Compounds EFSS Security Concerns even for Hybrid Cloud

If a company is concerned about the security ramifications of having data stored in the cloud and chooses to use some type of on-premises hybrid storage for EFSS, they will have another challenge. Since the copy stored on the on-premise storage will be considered the copy of record, they will need to put it on some type of reliable storage. In many cases, this will result in the purchase of an additional storage system just for this requirement. And although duplicating everyone's data to a local file server will have less of

an impact than duplicating it to a public cloud server, there is still an impact on the environment – especially during the initial migration. There also will be the duplication of data from the on-premises storage system to the user devices (laptops, tablets, smartphones).

One of the other challenges with having duplicates in multiple places is version control. Without aggressive file locking techniques, it's very easy to create multiple versions of the same file, each of which have changes from different people.

The model of synchronizing everything to a central location and then synchronizing it again to other remote locations works well for consumers who are sharing small amounts of data across varying Internet connections. But using that same model within an enterprise has different ramifications, including the storage costs and complexity of storing the additional duplicates, as well as the security risks of constantly creating duplicates on local or remote machines. Duplication quite simply increases your security risks.

Storage Swiss Take

What if enterprise users could directly share a user's file from its original location without creating an additional copy? (Think GoToMyPCTM, but for files.) If a file could be shared from its original location – whether file server or desktop – this would work for all types of files. This model is built more for the corporate environment, where inter-desktop communication is a lot easier than two consumers sharing files from their laptops over the Internet. It solves the problems above of creating duplicates, supporting the bandwidth required to copy the data around, and the unproductive management of the central copy stored on a file server or cloud server. By sharing from the source location, there is actually only one file and that resolves file locking problems. And finally, all of the data remains behind the firewall without requiring an additional file server on site.

Enterprise IT departments needed file sharing functionality, to stop users from

using consumer-grade file sync and share services without the consent or control of IT. It does appear, however, that in a rush to meet this need, companies designing such products have failed to take into account the differences between an IT department and consumers sharing data across the Internet. Taking this into consideration allows for a completely different design that doesn't have the same problems. Sharing files from the original location avoids the creation of duplicates and saves space, while also reducing cost and complexity. It also increases security by reducing the number of places a file can be accessed.

CHAPTER 4:

Now You Can Share Files Without File Sync & Share

By W. Curtis Preston, Senior Analyst

Enterprise IT departments have struggled with file sharing for some time. The traditional solutions were deemed by many users to be passé and not in keeping with modern workflows. This caused many users to resort to consumer-grade solutions, leading to "shadow IT," which creates many problems. Storage vendors and IT departments responded with products modeled after the consumer file sharing products. The problem is that those enterprise file sync and share solutions created as many problems as they solved. IT needs another way to solve this problem.

Those Pesky Users

For too many years, IT developed solutions around what made sense for IT and not what made sense for their users. Centralized file servers solve a lot of problems for IT, but they can't match the performance and convenience of a local hard drive. In addition, disk space that was once hard to find at the edge was suddenly available in spades. And, thanks to SSD-based laptops, high performance is at the edge as well.

Users wanted to use this local, seemingly unlimited, high performance storage.

Although users wanted to use their local storage, they also wanted to share their files with other people. Enter consumer-grade file sync and share products such as Dropbox. Users could easily share files with each other without involving IT or being forced to move their files to a file server. If they didn't have very many files to share, they didn't even have to pay for it. Users going beyond the free service didn't mind paying a few dollars a month for this functionality.

The dearth of these consumer-grade products represented a number of challenges for IT, and the answer seemed obvious. If users wanted a file sync and share service (the general term for products like Dropbox), the answer was an enterprise file sync and share (EFSS) service. The user experience was roughly the same as the consumer grade product, and IT could put some fences around it and support it.

EFSS Creates New Problems

As mentioned in other chapters, EFSS services create about as many problems as they solve. The reliance of most of them on a public cloud service creates jurisdiction issues, data residency issues, and law enforcement issues. In addition to the legal concerns surrounding the EFSS way to access your data, having the central copy of your data stored on a public cloud server also raises significant cyber-security concerns. If the datastore is compromised, a significant amount of your company's intellectual property could end up in the wrong hands. Apart from the well documented Target breach – many other security breaches substantiate the reality that the more content is shared/duplicated across networks, the risk of security breaches increases.

It is true that some of these services can sync to a private cloud and address many of these concerns, but it then creates a new requirement of a high availability service that will act as the central repository. And no matter where the repository is, the constant synchronization of files back and forth to multiple locations creates a significant amount of network traffic that cannot be ignored.

In the previous chapter we covered the fact that the very concept of file sync and share also is in opposition to one of the primary goals of IT, to reduce duplication of data. EFSS systems create duplicates of shared files in multiple places. Every duplicate of a file takes up extra space and consumes resources. Every duplicate also gives hackers an additional possible point of entry into your company's data.

Was EFSS The Right Response?

Users needed to share files, and they did not want to put those files on a centralized file server. IT didn't want users using a consumer-grade file sync and share (FSS) product. EFSS products seemed the natural solution. But EFSS products were essentially enterprise versions of the consumer-grade products that had very different design requirements than what IT would have. If you started from scratch with the need to share files without putting them on a centralized file server, would you end up with an FSS product?

FSS services like Dropbox™ were designed with the assumption that users sharing files didn't have direct access to each other's computers. It was one person on their computer in their house sharing files with another user on another computer in another house with two NAT routers between them. There was no way to directly connect two computers; the natural solution was a centralized cloud storage system that they could both access.

But that doesn't describe the typical use pattern of corporate IT. What if the solution facilitated direct network access to each other's computers? A centralized pool of storage would not be required. This would remove the security and legal concerns mentioned above, as well as removing the need for all of the duplicates that an EFSS system would create.

Storage Swiss Take: FileFlex

There is a solution to the problems and issues of using EFSS – it is a service called FileFlex. FileFlex is a secure, file sharing solution that allows users to access, share, stream and collaborate data with each other without using a centralized repository. Instead remote users access files directly from their original locations. This allows files to stay behind. the corporate firewall, and doesn't open them up to the security concerns of storing files on the third-party servers of an EFSS cloud.

It adds all the functions, features and benefits of EFSS to every file on your storage infrastructure , but keeps all your files on your own storage, behind your own firewall, under your own Government, Risk Management and Compliance (GRC), simply, at a fraction of the cost, turning it all effectively into a virtual private cloud.

First, because you access your files from their original locations, on your own storage and from behind your firewall you eliminate the issues inherent to storing your organization's files on someone else's computer. You minimize your threat surface, simplify your storage infrastructure and keep your governance, risk management and compliance completely under your control translating into a very strong security posture. Second, because your files are on your equipment located in your own facilities, you eliminate the issues of data residency, jurisdiction, third-party inspection and secret access by law enforcement. You comply with data residency

and privacy regulations such as HIPAA and GDPR. Additionally, since you don't need to purchase any expensive cloud storage it provides significant cost savings. Finally since it allows your users to access all of your corporate storage. you don't have the issues inherent with subsets and all corporate information is available as needed without syncing to local devices.

Even though the file remains in its original location, it is still accessible anywhere in the world to users that are authenticated against the system. Authenticated users can access files from any Windows, Mac or Linux computer, as well as any Android, iOS, BlackBerry or Windows tablet or

smartphone. Users accessing shared files on their computer access them as if they were local files. Computers sharing files appear as folders, under which you will find any folders or files shared from those computers. Not only can users access any file under this hierarchy, they can copy and paste files between any folders – even copying files between computers.

Although the files appear local, they are indeed not local – which is the whole point. Unlike EFSS systems, remote users do not have to set aside disk space for synchronization. There are also no file size limitations that some EFSS systems have. Also, unlike some remote access solutions, files are accessed in their native form, without any degradation such as compression. If any of the shared files are media files, remote users can stream them directly to their device, without having to download or synchronize the file. In fact, downloading can be prohibited by sharers as required.

In addition to allowing remote users to access file inside the network, it can also automatically bring their remote data into the network. Photos or videos they take on their smart phones or tablets can be automatically copied to the appropriate place inside your firewall.

IT administrators also have control over the system. They control who is allowed to share, what they are allowed to share, and who they can share it with. It's easy to deploy and does not require a VPN connection. All data will stay exactly where it is and does not need to be synced anywhere to share it.

Administrators can allow users to create their own shared repositories or they can add file servers to the system, allowing FileFlex users to access those file servers from anywhere. There is a distinct audit trail that logs user activities and an advanced dashboard for IT to manage the system. Finally, choosing FileFlex does not mean new purchases of hardware as no new storage locations are needed. It is also easy to integrate FIleFlex into an authentication system, as it supports LDAP, Active Directory, and Single Sign-on.

As opposed to your EFSS solution, because FileFlex keeps files in their source locations on your own infrastructure and on-premise behind your firewall, they are already under your GRC framework and under your control with auditing, account management, integration into LDAP, non-repudiation and strong encryption from your own management console and managed by your own IT personnel.

Allowing users to directly access files from their original locations meets the same user requirements as an EFSS system without suffering the drawbacks of those systems. Users don't have to make room on their computers for synchronized folders and those folders won't create security risks by propagating duplicates. Add the enterprise administration and control features and you have a strong solution for your file sharing needs.

About Storage Switzerland

Storage Switzerland is an analyst firm focused on the storage, virtualization and cloud marketplaces. Our goal is to educate IT Professionals on the various technologies and techniques available to help their applications scale further, perform better and be better protected. The results of this research can be found in the articles, videos, webinars, product analysis and case studies on our website storageswiss.com

George Crump, Chief Steward

George Crump is President and Founder of Storage Switzerland. With over 25 years of experience designing storage solutions for data centers across the US, he has seen the birth of such technologies as RAID, NAS and SAN. Prior to founding Storage Switzerland he was CTO at one the nation's largest storage integrators where he was in charge of technology testing, integration and product selection.

Curtis Preston, Lead Analyst

W. Curtis Preston (aka Mr. Backup) is an expert in backup & recovery systems; a space he has been working in since 1993. He has written three books on the subject, Backup & Recovery, Using SANs and NAS, and Unix Backup & Recovery. Mr. Preston is a writer and has spoken at hundreds of seminars and conferences around the world. Preston's mission is to arm today's IT managers with truly unbiased information about today's storage industry and its products.

About Qnext

Qnext Corp. is a global developer of disruptive apps and private cloud technologies committed to simplifying and protecting your digital life through innovation, imagination and state-of-the-art software. Their solution, FileFlex was created in response to users need for accessible data but is better than the traditional enterprise file sync and share solution. It virtualizes file access to ALL the company's disparate storage infrastructure and devices. This enables any server, notebook, desktop, SAN, NAS, public, private or virtual private cloud to be available anytime, anywhere through a secure and private network and single dashboard. The file access virtualization technology behind FileFlex essentially takes the company owned infrastructure and turns it, in its entirety, into a private cloud. For more information, visit https://fileflex.com

Storage Switzerland, LLC