FILECLOUD

Enterprise File Sharing Best Practices

whitepaper

The key to successful EFSS implementation is the process. This white paper explores some of the best practices organizations can follow to maximize productivity by collaborating securely.

Executive Summary

The need to collaborate both internally and externally with colleagues and partners is apparent to any modern enterprise. Organizations are heavily investing in collaboration systems and technology. Today, very few workers go through their work day without using some form of collaboration tool. Achieving an optimal level of collaboration without compromising data security is giving IT teams sleepless nights. With the rise of the bring-your-own-device (BYOD) movement, data leakage and loss is a massive threat that demands a greater level of care. For any business handling customer information, data privacy is vital to business success.

It has been said time and time again that data is the lifeblood of any company. This requires creating a collaborative environment that is always accessible. File sharing is probably the most effective way to create a collaborative environment. To ensure everyone has access to mission-critical data at a moments notice, most companies mobilize data.

However, mobilizing corporate data on a large scale without a properly safeguarding the solution introduces significant security risks. It opens the network to external threats, malware, and data loss. It also can lead to a violation of regulatory rules. Even with the best intentions, employees can inadvertently cause irreversible damage to a business by simply trying to work more efficiently.

Despite the widespread challenges, Enterprise File Sharing and Sync (EFSS) implementations are expected to rise in the coming years. Organizations are realizing that EFSS solutions have to protect data and prevent corporate espionage by securing intellectual property (IP) that users may share or sync using these systems. As organizations plan to implementing EFSS, they understand that they also must establish the right security measures and controls. Due to the nature of enterprise file sharing, the security solution needs to be capable of extending to any place that information is shared.

In reality, collaborating securely is easier said than done, especially if the right infrastructure or solution is not in place. The key to a successful EFSS implementation is in the process. This white paper explores some of the best practices organizations can follow to maximize productivity by collaborating securely.

By 2022, 50% of midsize and large organizations in mature regional markets will use a content collaboration platform (previously known as Enterprise Sharing and Sync - EFSS) to implement document workflows and improve collaboration and productivity.

A Closer Look at the Challenges

While the methods may have evolved, file sharing is not a new concept for enterprises. From messengers to carrier pigeons, – humanity has been sending correspondence back and forth for centuries. Fast forward to the digital age, and now the most common transport system is email. The traditional method of File Transfer Protocol (FTP) is still widely used, as are varying cloud-based EFSS tools.

However, EFSS is not without its pitfalls. While it simplifies and accelerates file access, the potential for breaching an organization's EFSS network is alarming. If EFSS is poorly configured or allows accidental disclosure to the wrong individual, it can cause irreparable harm to the organization in the way of fines, and loss of trust between the company and its partners, clients, and customers.

The following are some of the key problem areas that may cause data loss when sharing files.

Stuck in the Past

Email was designed as a means of communication, not a collaboration or file sharing tool. However, it has managed to become the default file sharing system for most businesses. This is despite the fact that is was never designed to meet the strict security and storage requirements of the modern enterprise.

Reliance on an email-based file sharing system makes compliance with corporate governance rules difficult. It is virtually impossible to perform audits on content being shared.

Email attachments account for over 75% of all data stored on email servers. In this digital age, email storage requirements can easily exceed capacity.

Data Leakage

According to a Cloud Security Alliance survey, 91% of industry experts believe that data loss and data breach are the most critical threats to cloud security.

Corporate data information leaks can be a major problem for even the smallest of businesses. A 2018 data-breach report by Ponemon concluded that the average costs are:

$418

for each stolen or lost record containing confidential information

$3.86 MILLION

for a data breach

Managing this risk is essential to keeping intellectual property safe and revenues flowing. In the absence of a layered security approach that includes Data Leak Prevention (DLP) and controls for protecting corporate data, employees often copy data onto USB drives, email attachments, or consumer cloud sharing apps.

Shadow IT

When dealing with challenges such as file size limits or unstructured security authentication processes, frustrated workers often turn to consumer file-sharing solutions.

With the growing number of BYOD, the risk of under-secured mobile devices within the enterprise has never been more prevalent.

The telltale sign of shadow IT is when employees are making security-related decisions, that they shouldn't be making. This scenario unwittingly introduce critical security issues.

Files shared externally through third-party service providers increases the risk of data leakage and compliance violations. This risk is amplified when IT is not aware of it.

Compliance Risk

Whenever employees move corporate data outside the organization's firewalls, they expose it to significant compliance risks. File sharing tools and personal email systems have become ubiquitous in the business world.

Even in highly regulated industries such as finance, law, education, and healthcare, recent surveys have shown that 84% of business users send confidential or classified information in corporate email attachments. This includes Personally Identifiable Information (PII) which is regulated by the government and can incur penalties.

Of those businesses where users send confidential or classified information in corporate email attachments:

72%
compromise security weekly

52%
compromise security daily

A major reason for this violation occurs is because IT managers have a difficult time tracking the files shared internally and externally.

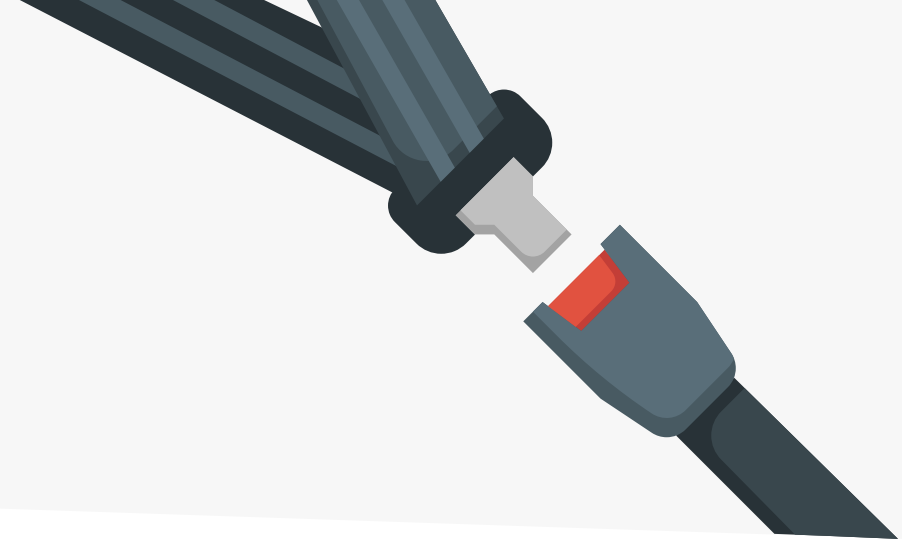
External Threats

Most business require that files can be shared externally. However, files shared freely are more susceptible to being hacked if proper security controls are not put in place. A recent research report looking at the most popular file-sharing services revealed that over 12 petabytes of data were exposed this past year.

For IT, ensuring the security of mobile devices has always been a challenge.

- Data transmitted over a public network is data at risk.
- Data residing on a stolen or lost device also represents a liability.
- When employees share corporate data using home computers or personal mobile devices, they risk it being intercepted.

Mitigate Risk by Employing Best Practices



Let IT Lead the Charge

The rapid adoption of cloud-based services has taken the security practices out of the hands of IT professionals. Employees have become more comfortable using cloud-based technologies to assist them in their work. This consumer-centric approach to IT puts individual employees in charge of corporate data. The result is an introduction of increasing risks. In an enterprise-centric approach, IT is at the forefront of file synchronization and sharing.

A solution controlled by IT is crucial since it minimizes risk while ensuring corporate policies are implemented and enforced. When IT is responsible for data access, appropriate control over confidential and sensitive information is almost guaranteed. This visibility enables IT to get ahead of issues, such as catching compliance violations or security vulnerabilities.

A key component of putting IT in control of the file sync and share (FSS) process is the ability to switch from the use of consumer-based FSS solutions to something more secure. It's important to understand that it isn't enough to eliminate the unauthorized programs.

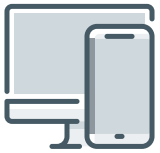
The new tool must be easier to use than the unauthorized solutions. Workers want an easy and accessible tool to help them share and manage files, and in the absence of an easy tool, they will likely resort to using email attachments and thumb-drives.

Choose an Enterprise-Grade Solution

With all the collaboration happening across both mobile computing and traditional network environments, IT and security teams have to find a way of effectively facilitating and controlling their information assets. At the same time, they must ensure that the inner workings of the technology remain transparent to users.

Unlike their consumer-centric counterparts, enterprise-grade file sharing solutions (EFSS) help manage the following issues:

Security



The user's ability to access files across multiple platforms.

Manageability

Most organizations typically adopt EFSS solutions to deter employees from sharing corporate data through file-sharing and storage services outside the control of IT.

Since EFSS platforms are built with security in mind, they come packed with features like authentication, storage, file transfer, monitoring and oversight. IT administrators can centralize file management and administration through EFSS as opposed to relying on users to keep track of unprotected files being shared over consumer-oriented public cloud services.

Align Security Needs with Compliance Requirements

Many industries are being included in government regulations and compliance is a more common concern. Such industries include:

- **Education** – with the FERPA regulations
- **HIPPA** – with the healthcare regulations
- **GDPR** – regulations for any company dealing with data on European citizens

Regulations on the storage and access of corporate files can be time-consuming for businesses. If you work in an industry bound by compliance regulations, then you already know that any file sharing solution must help you meet any applicable regulations.

No two organizations are the same; each has its own distinct business and regulatory requirements. Enterprise file sharing practices and solutions should have built-in compliance measures that align with their industry's regulatory requirements.

Keep it Simple

The key to maintaining secure file sharing is to adopt a solution that is easy for users and provides control for IT staff.

- Files should be easily accessible
- Users should be able to work from Android, iOS, Linux, Mac and Windows platforms.
- Users should be able to view files in a finder or an explorer, as with any other storage system.

Complicated file structures and permissions often result in immense inefficiencies. Employees end up spending too much time trying to figure out their way around the system as they try to share files.

The EFSS solution should also have a simple to use, and intuitive User Interface (UI). According to the Economist, employees who believe their workplace effectively utilizes mobile technology are more satisfied, creative, and productive at work.

Regardless of whether IT removes unsanctioned consumer-centric file sharing tools; if the alternative is less appealing, users will always choose the simpler solution without giving much thought to the security risks.

Choose An Integrated System Over a Separate-Point Solution

A standalone system that delivers files sharing is usually not enough to foster a rich collaborative workspace. A more integrated system reduces complexity by taking advantage of specialized applications. Your digital workspace must extend beyond file sharing to encompass a content collaboration hub that focuses on:

User mobility

Productivity

Workflow

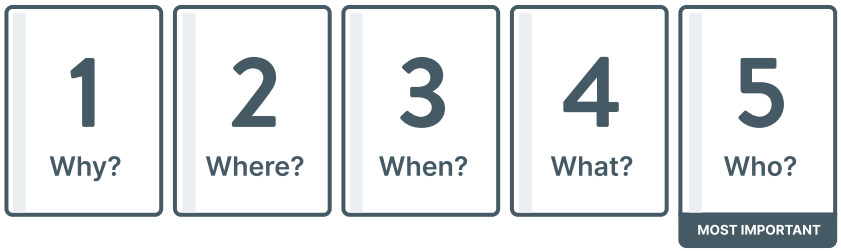
Security

Applications that can integrate with existing tools allows the organization to meet business objectives and boost the ROI from technology.

Consider Security Groups

A digital workspace requires a secure digital perimeter based on the user and their identity, not just device or location.

IT administrators need to enable or deny file access based on the **five W's** of access:



Identify the user base and ensure that users are properly categorized.

Assigning permissions to individual users can be a complicated process that results in a nightmarish overhead. A set of users in one security group should have similar file permissions across the board. Placing users in security groups with descriptive names makes it easier to map individual privileges and monitor data access patterns.

Take the Time to Plan Out a Strategy

When creating a file sharing strategy, center it around the following rules:

- What needs to be shared
- Who needs to have access to it

A well thought-out file sharing strategy should ideally include features like:

- Making the content available for a limited time or
- Enabling only authorized users access to content
- A solid file naming strategy coupled with a simple folder structure

When combined, these features improves efficiency while greatly reducing data breaches. A file sharing strategy is the first step towards managing data in accordance with legal, regulatory, and corporate policy requirements. Keep a plan that everyone can refer to and maintain consistency without allowing exceptions.

Facilitate Continual End User Training

An often overlooked yet crucial issue is the role end-users play in creating an environment where files are shared securely and efficiently. Employees should know the sensitivities of varying types of information and the risks associated with mishandling sensitive data.

After policies regarding unsanctioned file-sharing services have been developed, they should be effectively communicated to employees.

Anyone dealing with sensitive data should clearly understand what they can't share outside the organization. They should be educated on secure ways of sharing corporate information internally and externally.

Thorough and continual training is also the only way to guarantee that employees use the file sharing solution IT puts in place.

Plan for Failure

Unfortunately, even after employing best practices to share files securely, failure has to be considered. You have to be prepared for any possible data breach or loss by developing an effective emergency response strategy.

A good response plan will dictate who must be notified once a potential breach has been discovered or reported, in line with compliance requirements.

After the plan is created, it must be constantly tested and updated. Ensuring that your organization is equipped to respond to a data breach properly is a crucial component of your security.

Summary

Overall, enterprise file sharing and sync helps reduce security risks in the long term. With reduced business operating costs and enhanced user productivity, especially in the mobile workforce, the focus of enterprise file sharing applies not only to business practices, but also to IT and security mandates. If not implemented properly, the productivity benefits of EFSS can be outweighed by the risk of allowing large amounts of data to be easily removed from the enterprise.

If the best practices mentioned so far are important to you, than consider the FileCloud EFSS solution. It enables you to regain control of your data as it is shared.

FileCloud combines the benefits of collaboration and productivity with the security you require to protect your Intellectual Property anywhere it goes in the course of doing business.

About Us

A privately held software company, headquartered in Austin, Texas, USA, FileCloud is helping organizations thrive by providing hyper-secure content collaboration and processes solutions. FileCloud is used by millions of customers around the world, ranging from individuals to Global 1000 enterprises, educational institutions, government organizations, manufacturing companies, managed service providers and more.

1M+
USERS

3000+
ENTERPRISES

100+
RESELLERS

90+
COUNTRIES

13785 Research Blvd, Suite 125
Austin TX 78750, USA

Phone: U.S: +1 (888) 571-6480
Fax: +1 (866) 824-9584

support@filecloud.com
https://www.filecloud.com

CMS CENTERS FOR MEDICARE & MEDICAID SERVICES
REUTERS
US Army Corps of Engineers
NASA
COLUMBUS REGIONAL HEALTH
TOYOTA
Deloitte.

Copyright Notice