

➤ THE PITFALLS OF ONLINE FILE SHARING AND SENDING SERVICES FOR THE MEDIA & ENTERTAINMENT INDUSTRY:

Why I.T. finds them challenging and why you may be putting your business at risk by using them

Easy-to-use, readily-accessible, and consumer-oriented, online file sharing platforms such as Dropbox and Google Drive are, to end users, a pleasant replacement to older file transfer methods such as FTP. FTP is complex to use and requires IT intervention to make almost any change. The pain associated with FTP, which was developed in the 1970s, is one of the factors that opened the door for the rise of online file sharing services in the workplace.

Think about it: people are so accustomed to using browser-based, drag-and-drop file sharing in their personal lives, for sharing their documents, music files and photos with family and friends, that it was a no-brainer for many to use these same products instead of the company's official FTP server to send and share files with fellow employees, suppliers and customers. When given the chance to avoid IT headaches, many will jump.

Along with file sharing, for the sending large files, a series of consumer-focused tools have emerged such as WeTransfer to navigate around the size limitations of most email systems. For consumers who need to send large files to a friend that are too big for Gmail, tools like WeTransfer make it easy to do just that.

Just as with file sharing in the workplace, many business users will circumvent internal IT systems and use file sending services when they need to send a large file to co-workers, partners or customers.

These trends, of course, are making IT managers nervous (especially every time [major online file sharing data breaches](#) get publicized). Because now that users are self-migrating from FTP (or internal email systems), they're jumping on to these unsanctioned, public platforms, leaving IT out of the loop – with a pile of risks and challenges that companies can't afford to take. In some cases, EFSS (Enterprise File Sync and Share) systems including Box and Dropbox for Business are options for IT organizations to consider. These typically take a consumer-like offering and add additional management controls and, in some cases, more sophisticated security. EFSS solutions are widely deployed, and they are often considered a good choice for business documents. However, for a modern M&E company that is sending and sharing mission-critical content files, and massive video files at that, these EFSS systems aren't suited for their most important use cases.

Seven Pitfalls of Online File Sharing and Sending Services for M&E Companies

→ 1. No Acceleration

For all the promises of ease, access and user-friendliness of online file sharing and sending services, they fail to address the biggest bottleneck of all in moving large video files to other users: the transfer speed.

While employees might think they're circumventing an annoying process by avoiding an FTP interface, they're still left waiting for transfers to complete – and hoping they do so in time. Then their intended recipient must also wait for downloads on the other side. Why? Because these online file sharing services still rely on traditional TCP transfers that don't maximize network bandwidth. They are just as slow as FTP, but with a friendlier face.

→ 2. Flawed Security Models

[IT Security Guru](#) shares: "...Research has shown that 43 per cent of C-level executives say negligent insiders are the greatest threat to sensitive data. Instead of going through the red tape of IT procurement, provisioning, testing and security, employees are quick to download the latest app to access or share data. However, such a quick fix can have damaging implications on a company's most valuable corporate assets – its intellectual property and brand reputation...."

And it's no idle threat, according to [IT Security Guru](#):

Even if a company advertises that the content you upload into their system is encrypted in storage, you have no assurance whether your OFS (Online File Sharing) provider is following secure design principles. (Least privilege, Economy of mechanism/Simplicity. Open design, Complete mediation, fail-safe defaults [e.g., permission-based approach] and separation of privilege.)

Okay, let's say you get through all these hurdles and your OFS service is following secure design principles. Is your company's intellectual property and PII (Personally Identifiable Information) data now sitting in someone else's storage?

If you are using OFS it is possible that your company's security policies are being violated. For example, if you are sending PII data through an OFS provider do you know if you are in violation of privacy policy for your company? Freemium versions of the majority of these products DO NOT typically support critical security controls.

→ 3. Storage Lock-in

You can't choose where you want your assets stored. Online file sharing services use their own storage – and that could be anywhere, so your IT department has no control over the actual server where assets are stored.

→ 4. Closed Storage System

Additionally, because you have no control of where the content is stored, you cannot access this storage via other mechanisms. For example, you may wish to directly interact with files in your storage or move your files through an automated workflow that is outside or adjacent to your OFS storage.

→ 5. File Size Limits

As of July 2017, Dropbox has a file size limit of 20GB per file. That may seem like a lot but with today's 4K video cameras, you could exceed that limit quickly depending on FPS (frames per second), bitrate and codec.

→ 6. Poor Control and Visibility

Without direct ownership of or access to the storage and server management, online file sharing introduces a dangerous barrier to corporate visibility. Being able to restrict access and assign granular permissions to files makes sure that only the right people have access to move content. And, being able to view, track and audit activities ensures that if a breach occurs you can pinpoint its source.

→ 7. No Robust Transfer Mechanisms

Even if you decide that OFS meets all your needs, you can't afford to waste time starting at the beginning. With large files, Checkpoint Restart becomes of huge importance.

If a file transfer is interrupted due to internet connectivity or other network challenges, having to manually restart or worse having to start the transfer over from the beginning can be a nightmare in meeting deadlines – especially when there's no file acceleration.

Online file sharing and sending services are great for consumers and even for some simple business use cases – there's no denying that. But when it comes to mission-critical content and the complex workflows of modern M&E companies, these services aren't up to the challenge.

SIGNIANT'S MEDIA SHUTTLE is the easiest and most reliable way to send any size file, anywhere, fast. Media Shuttle is far and away the market leader in transferring large files fast and securely and is used today by more than 25,000 companies of all sizes.

Why Media Shuttle?

- **Speed** - Media Shuttle's proven file acceleration technology speeds up transfers over public and private networks up to 200 times faster than standard methods (such as FTP). Our patented technology practically eliminates latency, effectively utilizing available bandwidth.
- **No file size limits** - With Media Shuttle you don't have to worry about shipping hard drives, compressing files or breaking them into smaller files. Media Shuttle allows you to send any size file, anywhere, fast.
- **Rock solid reliability** - Media Shuttle comes with Checkpoint Restart, which automatically retries or resumes failed transfers. You'll also receive email notifications when files have been downloaded, so you'll never have to guess if your files went through.
- **Comprehensive security model** - Building on the core Transport Layer Security (TLS) built into the Signiant transfer protocol, Media Shuttle contains a variety of security features that adhere to the information assurance principle of "defense in depth". A defense-in-depth design strategy incorporates several security controls for a system so that multiple security failures must occur before an attacker can gain access to critical resources.
- Media Shuttle makes it easy to share files between people, between systems and to and from the cloud. There are **three different types of portals** that can be created to support almost any use case.
 - SEND portals allow for fast person to person file transfer.
 - SHARE portals make it easy to upload and download files within designated folders.
 - SUBMIT portals provide an onramp for users to submit files into automated workflows.
- **Role-based access** - Media Shuttle offers roles for three key user types in the organization – end users, operational administrators and IT administrators. Each user type has a tailored view that's made explicitly for their job function. Media Shuttle makes it easy to enable all users, whether internal or external, to access only the files and features they require.

- **CloudSpeX** dramatically lowers rejection rates associated with the receipt of improperly formatted files or incorrect file types, and helps to manage the volume and complexity of today's multiplatform delivery specifications. Unlike other solutions that validate file format compliance after the file transfer, CloudSpeX ensures that your specifications are enforced prior to delivery to save significant time and resources.
- **Metadata entry** allows end users to populate predefined fields with information describing the file they are about to share. The experience is fully customizable, offering system administrators the ability to define fields for any parameter – often things such as language or shooting location – to ensure that all of the necessary information is captured. The metadata remains associated with the file, making it easy for a person or process to take action upon receipt.
- **App-less transfers** - Authorized users are able to access their files from anywhere, on any device, without any special software on their computer. While most users engage with Signiant systems via an installed application or browser plug-in to take advantage of accelerated transport, there are some situations where this is impractical. By accommodating users who want to use a mobile device or are unable to install software, Signiant enables adoption across the entire media ecosystem with completely clientless access.
- **Storage independence** - With Media Shuttle, you have the choice of storing your content on-premises or in cloud object storage. This includes the flexibility to allocate all the same storage locations, or the choice of allocating different storage locations for each of your portals. Ultimately that means you have full control of where your files are at all times, and the flexibility to easily change that storage allocation at any time not locking you into any one provider.
- **APIs** - Media Shuttle provides two APIs for customers who want to implement automated computer control of certain Media Shuttle functions:
 - The administration API enables automation of repetitive tasks like portal creation, storage assignment, and user creation. Customers are successfully using this API to replace manual processes, and to replace automated tasks associated with older technology (e.g. scripted FTP server setup).
 - An API for 'system to person' automation is now available so that IT organizations and integrators can create simple, automated 'click here to download' workflows from their in-house and commercial DAM (Digital Asset Management) and MAM (Media Asset Management) systems.

If your team is using services like Dropbox or Google Drive to share corporate assets or WeTransfer or HighTail to send large media files, it's time to consider [Media Shuttle](#) for secure, reliable, accelerated file transfer.

Media Shuttle

THE EASIEST WAY TO SEND AND SHARE FILES ANYWHERE FAST

Media Shuttle is a hybrid SaaS solution that allows media professionals to quickly transfer any size file anywhere in the world.

Learn more:
www.signiant.com/mediashuttle

Manager+Agents

AUTOMATED SYSTEM-TO-SYSTEM FILE MOVEMENT

Manager+Agents is an enterprise software solution for automated delivery of large files across geographically dispersed locations.

Learn more:
www.signiant.com/manageragents



EASY, FAST SYSTEM-TO-SYSTEM FILE TRANSFERS

Jet is a powerfully simple SaaS solution to automate recurring file transfer jobs between global locations and partners.

Learn more:
www.signiant.com/jet



MOVE FILES INTO AND OUT OF CLOUD OBJECT STORAGE

Flight is an auto-scaling SaaS utility that accelerates the transfer of large data sets into and out of cloud object storage.

Learn more:
www.signiant.com/flight



We were using a range of other products like WeTransfer, Dropbox and Box. We had so many different ones that were either client specified or just set up for specific reasons that it was very difficult to manage or help people if they had an issue.”

~**Michael Ball**, Post-Production Supervisor, **Accord Productions**

ABOUT SIGNIANT



Signiant's enterprise software provides the world's top content creators and distributors with fast, reliable, secure access to large media files, regardless of physical storage type or location. By enabling authorized people and processes to seamlessly exchange valuable content – within and between enterprises – Signiant connects the global media supply chain. **Find out more at www.signiant.com.**