citrix

White Paper

Think beyond file storage to accelerate business efficiency

Empower employees with fast, secure access to any file from any device

How to give employees fast, convenient access to files — while keeping your data secure

If employees can't easily access any file from any device, they will go around your IT policies and buy their own cloud storage. To prevent shadow IT, you must provide a file-sharing tool that combines the security your business needs with the convenience that users demand.

End the tug of war between user convenience and IT security

A few years ago, improving business productivity meant allowing employees to use their smartphones for work.

Now, employees expect to work from a greater number of devices and locations. The average employee uses up to three devices each day for work-related tasks.[1] For example, they may use their smartphone to check email over their morning coffee, update a presentation on their tablet while they are on the train, and access files from their home laptop on days when their kids are sick.

However, despite the freedom to use whatever device is convenient at the time, many employees have a poor experience when they move between devices. They often lack access to essential applications from their mobile devices. Or, a file they save on their office hard drive may not sync with their mobile devices. This lack of access is not just frustrating, but can have a massive impact on business productivity.

Are employees putting your data at risk?

Today's employees need fast and easy access to files — no matter which device they are using or where they are located.

If your existing file storage doesn't give employees this fast and easy access, they will go around you to procure cloud storage that makes files accessible across all their devices. Because these personal storage solutions often exist outside your IT policies, they fail to meet industry compliance rules for data privacy and security.

If you don't gain visibility and control over this growing data sprawl, your risks of a breach will only increase. So it's no surprise that data loss and leakage and data privacy are among the biggest cloud security concerns today.[2]

Accelerate business efficiency while protecting your data

You no longer need to choose between user convenience and data security. Today's file sharing tools have moved beyond basic cloud storage to offer security that's both rigorous and flexible. This allows employees to access files from any device and location — while you maintain strict security standards.

With the right file sharing solution, you can:

- Give employees anywhere, on-demand access to files
- Boost productivity with automated workflows
- Store data flexibly in public and private clouds
- Improve your data security
- Make your data more available and reliable

3 keys to boosting business efficiency

1. Automated workflows

Companies often rely on manual processes that are slow and inefficient. For example, a car insurance rep may visit the site of an accident, gather all necessary information, take a few photos, and then return to the office to complete an accident report to support the customer claim. If the person who needs to review the report is on vacation, the claim can get delayed for weeks. This can frustrate the customer and motivate them to look elsewhere for insurance when it's time to renew.

Automating this workflow could expedite the entire process. Using a mobile device, the rep could complete the report and file it while still at the accident site. The claim could then be automatically sent to a supervisor for review and approval, and a signature could even be collected to ensure the claim is processed promptly.

Here are five more reasons why you should automate your workflows:

- Complete tasks faster
- Reduce the number of steps in a process to remove inefficiencies and find cost savings
- Close deals in less time with automated approvals and legally-binding e-signatures
- Maintain audit trails — without manual intervention
- Streamline employee operations without requiring a dedicated IT team

2. Give employees the flexibility to use any device from any location

Employees who use multiple devices to view, edit, and share files often encounter barriers. For example, personal file sharing services can only access a limited number of networks.

If employees are outside of a network's range, they may not be able to open a file. Then, they might miss deadlines or fail to make decisions because they don't have the information that they need.

Your file sharing solution should allow employees to access all of your data sources from a single, central location–no matter which devices or networks they are using. With just a few clicks or swipes, they should be able to access files on SharePoint, OneDrive for Business, your network file drives, and your content management system. This will help you boost productivity without tethering employees to a specific database, network, or computer.

3. Data storage choice

If you lock your data within a private network, employees will have a hard time accessing files when they work outside the office or on multiple mobile devices. Employees who can't get what they need may ignore your IT policies and upload files to any convenient location–often a public cloud that doesn't meet your security and compliance requirements. The average employee uses 36 cloud services[4] at work, most of which don't follow your IT policies.

You can gain control over your data, while making work easier for employees, by choosing a file sharing solution that gives you flexible storage. Public cloud storage can enhance your agility and simplify your IT management. It also helps you reduce your costs, as you won't need to invest in hardware or pay for the bandwidth needed to share large files. Meanwhile, you can continue to use your private cloud storage to protect your regulated data.

85% of data breaches start with a human error

How to keep your data secure (no matter where it resides)

Apply access controls

Almost 85 percent of data breaches start with a human error.[4] For example, an employee may email a sensitive document to someone who isn't supposed to view it.

Your file sharing solution should give you control over who can view your data–both inside and outside your company's walls. Here are some security features that will help you protect your files:

- Role-based access controls that let you specify who can view, print, edit, and share documents
- Seamless integration with your company directory services to simplify authentication and end-user provisioning
- The ability to revoke access to files, in case an employee sends sensitive information to the wrong person
- Restrictions on the number of times someone can upload or download a file
- Email and file encryption
- The ability to block access based on someone's network location

Protect your company's devices and data

Lost or stolen mobile devices significantly increase your risks of a data breach. Your file sharing solution can be your first line of defense when an employee's device goes missing. Choose a solution that lets you remotely wipe files from devices that are lost or stolen. It should also allow you to lock devices that are not in use, require employees to enter passcodes to view content, and apply data expiration policies to keep your files secure and under control.

Gain visibility into your mobile data

Although most companies have policies around accessing and sharing files, 27 percent of employees are unaware of them.[5] This lack of knowledge can cause employees to take risks with your data, such as uploading it to a questionable cloud service or forwarding it to an unauthorized user.

Your file sharing solution should give you visibility into what employees are doing with your data. It should provide real-time tracking of user activity, so you can spot vulnerabilities and minimize your risk of data leakage. Your solution should also allow you to run custom reports, so you can meet your company's data policies and compliance requirements.

Work efficiently and securely — from anywhere — with ShareFile

ShareFile gives employees the productivity and collaboration tools they need to work from any device and location. Employees can share documents, collect feedback, get approvals, and more — while you maintain tight control over your data.

With ShareFile, you can:

- Access all of your files through a single, secure portal
- Gain control over data sprawl by providing effortless access to data stored on your company network from any device
- Automate your workflows to achieve greater efficiencies with fewer errors
- Boost employee productivity without compromising your security
- Take advantage of flexible storage that allows you to divide data between public and private clouds
- Integrate file sharing with your existing business productivity tools, including Office 365

Next steps

If employees can't easily access any file from any device, they will go rogue and upload your data to unauthorized cloud services. To prevent data leakage, choose a file-sharing solution that combines the security, flexibility and control that your business needs with the convenience and productivity features users demand.

Visit citrix.com/sharefile to discover more ways you can accelerate business efficiencies while keeping data secure.

Sources:

[1] CapGemini, Transformation Journey with Digital Employee Experience - Digital Office, 2017
[2] Cybersecurity Insiders, 2018 Cloud Security Report
[3] Skyhigh Networks: 12 must-know statistics on cloud usage in the enterprise, March 9, 2017
[4] Computer Weekly: Security professionals name top causes of breaches, August, 25, 2017
[5] Igloo Software: State of the Digital Workplace 2018, May 2018

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States