Cloud storage buyer's guide

FOR SMALL BUSINESS

sponsored by tresorit

Table of contents

Why should you read this guide?

You've used Dropbox yourself and it seemed really fast. How about live collaboration with Google Drive – sounds useful, right?

If you Google *"best cloud storage for small business"*, you'll find plenty of articles listing services you could take a look at. There's also some vague advice about reading the fine text before you click "I accept". But what's the best cloud storage for YOUR business and its unique set of needs? How do you adopt the best product and cloud policies for your organisation? If you don't have a policy then your staff may well be using such tools, sharing sensitive information with others without your knowledge or control.

Another issue is that of security – after all, stories of breaches keep making the news. Cloud providers, having realized the market potential, claim to be absolutely secure. But is that true? It's hard to tell without IT security expertise. Deploying a cloud service is a significant undertaking. Files need to be transferred, users trained and adoption monitored. Just like choosing insurance providers or accounting software, you must think this one through.

But how? Manually testing each and every cloud provider is not feasible. The general information in the press rarely answers your questions.

We've created a simple checklist to help figure out what your business needs to succeed. To help choose a service that fits the bill, we've also compared the most popular ones on page 10*.

**The comparison is based on objective criteria. All information was compiled from publicly available sources and manual testing of each service. If you need any help or have further questions, feel free to reach out.*

Step 1

Decide how much security you need

Cybercrime is on the rise. Government surveillance programs fill headlines. There are more ways to leak business data accidentally than ever before. All the while, your employees don't take the necessary steps to protect company data. Small businesses face the biggest risk. They lack sophisticated protection, and rarely take necessary steps to prevent a breach. Sadly, less than 40%* can survive one.

All major cloud storage services ***claim to be secure.*** But they don't tell you that there can be huge, practical difference between one method of security and another. Cases in point are the difficulties Dropbox faced recently, when millions of account details were allegedly breached through its integration with third party apps. Google Drive itself has had trouble ensuring user privacy. Its privacy policy states Google can *"use, host, store, reproduce, modify, create derivative works, communicate, publish, publicly perform, publicly display and distribute (your) content".*

LOOK FOR TOP TIER SECURITY IF YOU...

✓ store strategic documents, high-value intellectual property or information which, if leaked, could affect your reputation

✓ handle sensitive client data like passwords, health records or credit card information

✓ work in an industry which regulates how data should be managed

✓ suspect subpoenas might be issued to gain access to your data or that of a client

✓ work in an industry frequently targeted by cyber criminals, like finance or retail

✓ do not feel government agencies like the NSA or UK's GCHQ should access your data

Features that guarantee a service is secure:

Strong encryption at rest and in transit

Most data management regulation sets a minimum "key strength" of encryption at rest on the provider's servers and in transit. However, neither protective layer guarantees your provider will keep your data safe in case of a bug, subpoena or the data collection by a government agency.

End-to-end encryption during storage and sharing

Encrypting data before it leaves your device prevents your provider - or anyone with access to their systems - from viewing the files you store or share. It is the only known protection against your own service provider, ensuring it cannot comply with subpoenas or government surveillance.

Data storage outside the USA

Edward Snowden's revelations about government spying showed that storing data with US-based providers opens ways to access your data without your consent or knowledge. Strict privacy law in the European Union or Switzerland grants you much higher legal and practical protection.

* 17 National Cyber Security Alliance. "America's Small Businesses Must Take Online Security More Seriously." – September 2013.

Step 2/A

Consider what you need cloud storage for

Before picking a service, you need to think about how you will use it. Is accessing files on the road important to you? Do you share data with anyone outside your organization? Each service has distinct advantages when it comes to backup, sync or collaboration. The following 4 questions will help you pick the right one.

Do you need to work and edit files from anywhere?

The need for accessing company documents anywhere often motivates the move to the cloud. The question is – do you need to edit files or collaborate on the road? Or are you content with only working from the office computer?

LOOK FOR MOBILITY IF YOU...

- ✓ need to access and edit files offsite, where no company computers are available
- ✓ support a Bring Your Own Device policy, and provide access on devices that don't belong to the company
- ✓ run the risk of losing devices which store important data
- ✓ take photos or create videos on a mobile device that you want to access and back up

Features that support secure mobility:

Applications available for all platforms you use
Providers offer native apps on a host of platforms – make sure they have your needs covered.

Edit and sync files from mobile apps
Some providers offer a host of productivity features on mobile, while others don't allow you to edit files at all.

Account security for mobile devices
Additional layers of security should be added to all accounts to prevent unauthorized access in case a device is lost or stolen. This includes 2-Step Verification, a passcode lock and the ability to wipe a data remotely.

Step 2/B

Do you need to share files and collaborate with others?

Some businesses only need to backup their data and access it occasionally on the road. But when you work with colleagues on the same file, looking through dozens of email attachments to find the latest version can get old.

LOOK FOR COLLABORATION IF YOU...

- ✓ work with colleagues on reports, contracts, presentations or other documents
- ✓ share files with clients or business partners outside the organization
- ✓ collaborate with others on documents at the same time
- ✓ have partners who insist on due diligence before signing up for any service you'd like to use

Features that make collaboration efficient:

Send files or folders via direct links

Sometimes you only need to share a single file with someone. Business partners may also refuse to install new software before their IT departments had a thorough look at it – which could take weeks. In this case, you can send a link and skip the process altogether.

Activity feeds and version history

When collaborating with others, seeing who's doing what at a glance is useful, especially for larger teams. Services often couple this activity history with version history, so you can roll back to any previous version of a file easily.

Live, in-app collaboration

With certain services, several collaborators can simultaneously edit the same document, add comments and chat – generally in the web browser.

> *We upload the documents to the cloud for the client. It appears immediately on their laptop, so we could be talking on the phone and look at it together rather than doing it by post and waiting days.*
>
> **Guy Applebee**, Alpha Independent Mortgages

Step 2/C

How much control do you need over documents you collaborate on?

You often need to share sensitive data outside the borders of your team or organization. Setting, modifying and ultimately revoking access to these files can make or break your business when a project ends or a contract expires. Any customer data is further regulated by law, which compels businesses to protect it with adequate encryption.

KEEP CONTROL OVER SHARED DOCUMENTS IF YOU...

- ✓ share customer data outside the organization or with team members
- ✓ exchange contracts, financial reports, product designs or other sensitive documents with business partners or customers
- ✓ need to control copying, editing, emailing or sharing of sensitive documents
- ✓ work with other companies on highly sensitive, customer-centric projects like Mergers & Acquisitions
- ✓ anticipate the need to revoke access to documents you shared - like when a contractor's agreement is set to expire after a project

Features that keep you in control:

Granular permission levels

Granting limited access to some collaborators can mean the difference between a breach and smooth collaboration. Modifying or revoking permissions at a moment's notice ensures you react to changing circumstances.

Security settings for direct links

Setting direct links to expire after a certain time or number of downloads decreases the chance of a leak. Password protection is another common security measure.

Digital Rights Management

Security in transit and at rest on the provider's servers is great. But when a document is downloaded to a device, that protection evaporates. Digital Rights Management protection travels with files, wherever they go. It also lets you stop your collaborators from forwarding, printing, copying or editing the content of your confidential files.

Step 2/D

Do you want to bring your whole team or organization to the cloud?

Employees often put business data at risk by bringing their own, uncontrolled file storage and sharing solutions to the workplace. Choosing the right cloud solution can re-establish your control over critical data.

LOOK FOR CENTRAL ADMINISTRATIVE FEATURES IF YOU...

- ✓ want to limit access to business data for certain employees or teams in your organization
- ✓ work with a team distributed across locations and active on several devices
- ✓ need an audit trail to your data to make sure you can comply with regulations or legal requests

Features to monitor your organization’s usage and maintain security:

Admin dashboard

When managing a team or business, it’s imperative to see important stats like logins, devices used and accessed documents at a glance.

User groups

Assigning users to different groups can help to control access to business data across your organization.

Access policies

Deciding which devices should be used, and where users are allowed to log into the company account helps you to safeguard business-critical documents.

> *The deal involves nearly a hundred individuals from several contracting firms. If a contract expires, we need to ensure we can revoke the company’s access to deal documents.*
>
> **Robert Frodsham**, Little Venice Partners

Step 3

Know your organization

Some cloud services focus on large enterprises, while others target individual users. Now that you've figured out what exactly you need cloud storage for, it's time to make sure the service you choose will meet your organization's demands.

Answer the following 3 questions,
then use the comparison table under Step 4 to pick a winner.

? How tech savvy are your users?

Ease of use varies wildly across cloud storage services. To avoid pushback, you need to make sure your end-users are comfortable working with the service you choose. Some providers also offer in-depth training for new firms and their employees.

? Do you have internal IT expertise?

IT expertise is often required to set up a cloud system effectively and what's even more important, securely. If the service you choose isn't too user friendly, IT will also need to support staff to ensure the new service is adopted.

? How much time do you have for the migration?

Switching to most services requires you to move or rearrange your existing folder structure. Some allow syncing any folder, regardless of its place on the hard drive.

> *Our directors have varying levels of computer knowledge, so a simple, easy to use solution was needed.*
>
> **John Wilcox**, Yeldham Transport Collection

Step 4

A comparison of top cloud storage services

	Box	Dropbox	Google Drive	Microsoft OneDrive	SpiderOak	Tresorit
	For larger organizations looking for fast, efficient collaboration. Middling security.	Reliable sync service for teams that don't care too much about security.	Works well with other Google services. Privacy of stored documents is questionable.	Cheap, bulk storage without bells and whistles. Offers the least security.	Reliable, if unwieldy backup solution. Secure, unless you use it on mobile or share documents.	Collaboration with several layers of proven, Swiss security.
Step 1 SECURITY						
Encryption at rest and in transit	✓	✓	✓	only in transit	✓	✓
End-to-end encryption for storage and sharing	✗	✗	✗	✗	only for storage	✓
Proven security	✗	✗	✗	✗	✗	$50,000 hacker bounty, 1000+ unsuccessful attacks
Server location	US, global	US	US, global	US, global	US	European Union
Step 2/A MOBILITY						
Edit and sync files from mobile apps	✓	✓	✓	✓	✗	✓
Remote wipe of mobile devices	✓	✓	✓	✗	✗	✓
2-Step Verification and Passcode Lock on mobile devices	✓	✓	✓	only 2-Step Verification	only 2-Step Verification	✓
Step 2/B COLLABORATION						
Send files or folders using direct links	✓	✓	✓	✓	only files	only files
Activity feed	✓	✓	✓	✓	limited	✓
Live, in-app collaboration	only in Box Notes	with Dropbox Badge, in Office documents	in Google documents	✗	✗	✗

	Box	Dropbox	Google Drive	Microsoft OneDrive	SpiderOak	Tresorit
	For larger organizations looking for fast, efficient collaboration. Middling security.	Reliable sync service for teams that don't care too much about security.	Works well with other Google services. Privacy of stored documents is questionable.	Cheap, bulk storage without bells and whistles. Offers the least security.	Reliable, if unwieldy backup solution. Secure, unless you use it on mobile or share documents.	Collaboration with several layers of proven, Swiss security.
Step 2/C CONTROLLED SHARING						
Granular permission levels	✓	✓	✓	✓	✓	✓
Security settings for direct links	✓	✓	limited	✓	✓	✓
Digital Rights Management	limited to documents in browser	✗	✗	✗	✗	✓
Step 2/D ADMINISTRATION						
Admin dashboard	✓	✓	✓	✓	✓	✓
User groups	✓	✓	✗	✗	✓	✓
Access policies	Device restrictions	✗	✗	✗	Device restrictions	Device and location based restrictions
STEP 3 BUSINESS SPECIFIC						
Data migration	Need to manually move all files to Box Sync folder, or use FTP for bulk file transfer	Need to manually move all files to Dropbox folder	Need to manually move all files to Google Drive folder	Need to manually move all files to separate OneDrive folder	No need to manually move folders, they can be synced in place	No need to manually move folders, they can be synced in place
Ease of use*	Medium	High	High	Medium	Low	High
Deployment support for SMBs	Training videos	Training videos	FAQ	Only for large clients	FAQ	Training videos, free training for staff
PLATFORM SUPPORT						
Desktop OS supported	Windows, Mac	Windows, Mac, Linux	Windows, Mac	Windows, Mac	Windows, Mac	Windows, Mac, Linux planned for Q2, 2015
Mobile OS supported	iOS, Android, Windows Phone, BlackBerry	iOS, Android, Windows Phone, BlackBerry, Kindle	iOS, Android	iOS, Android, Windows Phone,Blackberry	iOS, Android	iOS, Android, Windows Phone, BlackBerry
Secure browser access	✗	✗	✗	✗	✗	✓

* based on ratings in major app stores and established review sites

Step 5

Build your action plan

Decide on the the number of seats

Do you want to use the new service with team members, or roll it out to the whole organization?

Evaluate your current storage, backup and file sharing solution

Your current infrastructure dictates how fast you can migrate data to the new service. Some setups allow you to switch with a click, while an SFTP needs more careful rearrangement of data.

Forecast budget & time requirements, get approval

Based on your current system and the service you choose, create a rough estimate for budgetary needs. Don't forget to factor in what you save in upkeep costs. After this, involve the rest of the company in the decision to make sure you have buy-in.

Run trial

Select a smaller project you can use to run a test of the service. Use the free trial time and a small group of core users to see how the service holds up under stress, how easy it is to use, and whether you should expect to support employees when you roll it out company-wide.

Get the lay of land

Create a spreadsheet matching data to the employees and business associates who can access them. Make sure to include the two most sensitive types: customer information and intellectual property.

Set up roles and permissions

Once you've identified your assets, it's important to review levels of access. It's important that these are refined, limiting access and edit of important data to authorized staff.

Onboard new users

Based on your trial experience, make sure your users know enough get started. This is crucial - lack of adoption is a primary cause of failed cloud deployments. Service providers often offer training of their own. Make sure to take advantage of this.

Monitor usage

Monitor usage via an admin dashboard in the critical first 3-4 weeks after rollout. Tackle lack of activity at any employee who should be actively using the service. The level of support your service provider offers is key. Troubleshooting any problems ensures rollout goes smoothly.

About Tresorit

Combining security with simplicity

You used to have two choices. Spend countless dollars and hours to set up a clunky but secure service. Or hope for the best and use Dropbox. **Use Tresorit, and you won't have to choose again.**

Tresorit's patent-pending security encrypts files on your device. With its **zero-knowledge system**, only you can grant access to your data. Decide if collaborators can email or copy files. Access to documents can be revoked in an instant, even if someone saved them to a device.

To prove its security, Tresorit posted a **$50,000 bounty** and invited hackers from around the world to hack its system. The prize has never been claimed.

> *Transitioning to Tresorit after one of the partners' Dropbox accounts was compromised couldn't have been simpler for us. Their customer service is some of the best I've ever experienced.*
>
> **Robert Frodsham**, Associate, Little Venice Partners

Try Tresorit's simple, secure sharing

Ready to go in 5 minutes, while your team continues working the way it always has. Regardless of the service you currently use.

Get started

tresorit

www.tresorit.com