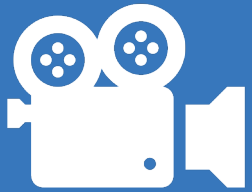


Cloud Backups Have an Expiration Date



Welcome!



Our webcast is being recorded.

Keep an eye out for the on-demand recording & slides in your inbox.



Submit your questions in the chat anytime.

And stay tuned for our Q&A at the end!

Meet the Presenters



Leif Watkins

Sales Director
ioSafe



Nichole Kucher

Digital Marketing Manager
CDSG

ioSafe Shields Your Data from Disaster

- We aim to safeguard your data from unforeseen disasters
- Fireproof and waterproof storage
 - NAS and direct-attach products
 - Fireproof 30 minutes at 1550°
 - Waterproof up to 10 feet for 3 days
- Local data for privacy, speed, and control
- Cloud-friendly for flexibility
- Data Recovery Service (DRS) available



Today we're talking about

1. Cloud storage

How files are stored, advantages, disadvantages

2. Cloud data recovery restrictions

Common cloud storage services and data recovery expirations

3. How to extend the lifetime of your cloud-stored data

Building your custom backup plan to make sure your files aren't lost



Cloud storage: What's it all about?

Cloud storage in a nutshell

Cloud storage

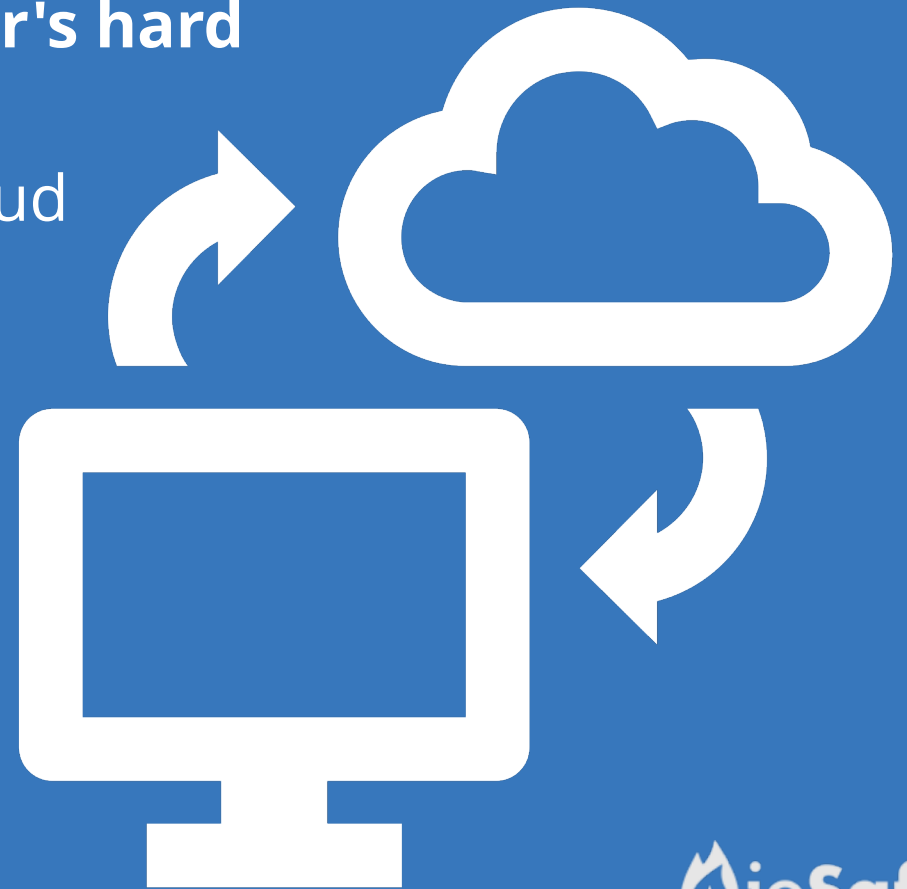
Saving data to an off-site storage system (computer hardware) maintained by a company you employ to store that data



How does cloud storage work?

Instead of storing your data to your **computer's hard drive** or other local storage, you **save data to a remote location** maintained by your cloud service provider of choice

Ex: Google Suite, OneDrive, Box, iCloud, etc.



Advantages of cloud storage



Safety



Scalability



Collaboration



Do you maintain ownership of your data when moved to the cloud?

Yes. However, your cloud provider has control of your data. They might hold your data to comply with regulations or delete your data based on retention policies to save on storage space.

Disadvantages of cloud storage



Instability



Cost



Privacy



Why is the cloud unstable?

Since cloud-based solutions depend on the speed of your internet upload and download speeds, having high latency can impede you from accessing the data in real time.

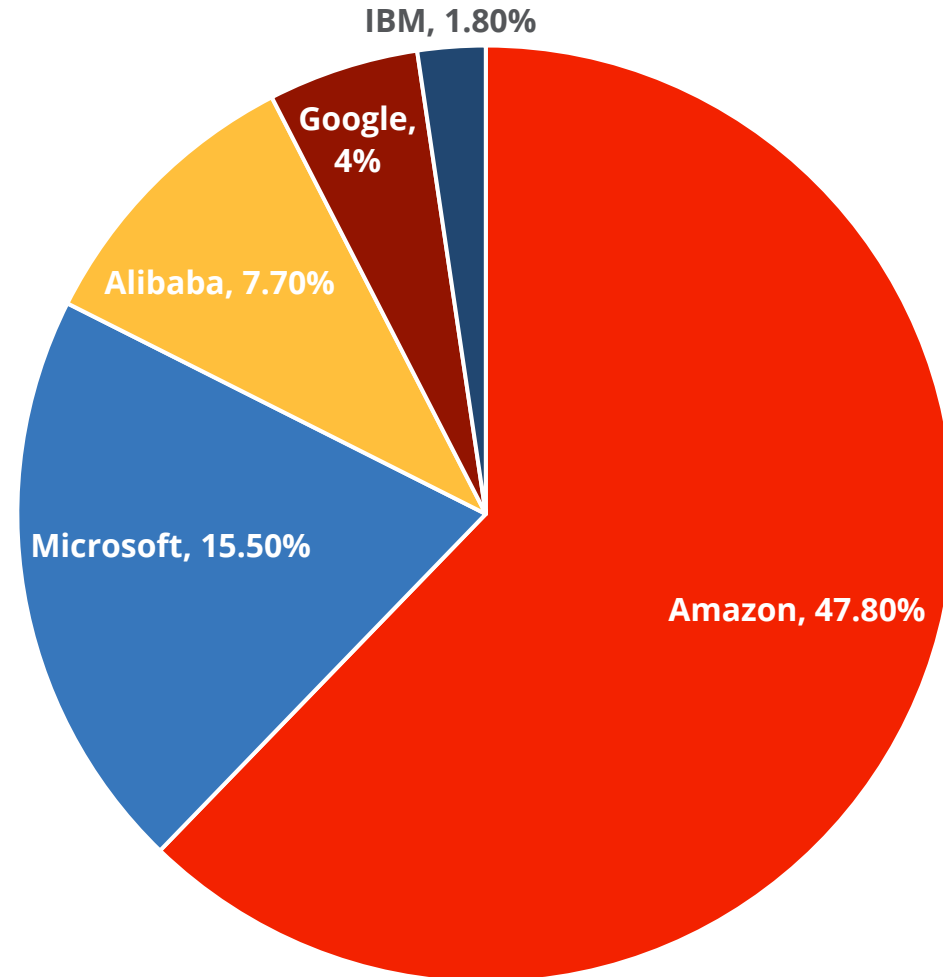
Cloud storage risks

- **Cloud security is tight, but it's not infallible.**
- **Cybercriminals can get into your files**, whether by guessing security questions or bypassing passwords.
- **Privacy** is one of the biggest risks with cloud storage.
- Even your data isn't stolen or published, it can still be viewed.



Amazon reigns supreme

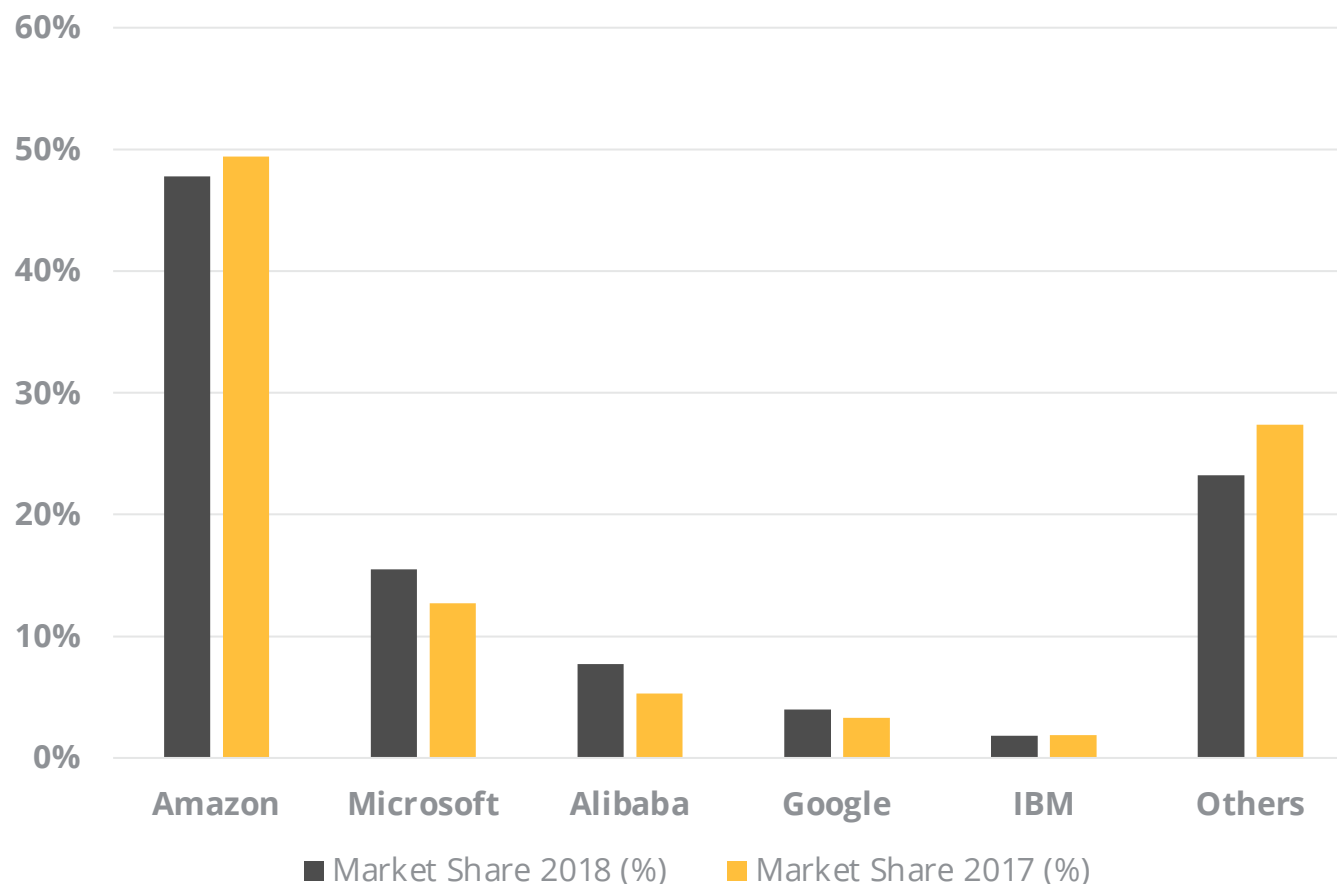
Amazon owns nearly **half of the world's public-cloud infrastructure market.**



Source: <https://www.forbes.com/sites/jeanbaptiste/2019/08/02/amazon-owns-nearly-half-of-the-public-cloud-infrastructure-market-worth-over-32-billion-report>

Global market shares

These top 5 cloud infrastructure providers accounted for nearly **80% of the global market in 2018**.



Source: <https://www.forbes.com/sites/jeanbaptiste/2019/08/02/amazon-owns-nearly-half-of-the-public-cloud-infrastructure-market-worth-over-32-billion-report>

Is relying on cloud storage
worth the risk?





Cloud data recovery restrictions

Cloud files aren't forever

And I almost learned that the hard way





Popular Cloud Storage Services

- Google G Suite
- Microsoft Office 365
- Microsoft OneDrive
- iCloud
- Box
- DropBox

Let's look at these 3!

Google G Suite

What happens to your files **after they're deleted?**

	Gmail	Google Drive	Google Calendar	Google Contacts
Kept in Trash	30 days	30 days	No	30 days
Permanently Deleted from Trash	After 30 day period ends	After 30 day period ends**	N/A	After 30 day period ends
Restore After Deletion?	Yes, up to 30 days after permanent deletion, through this Gmail Message Recovery Tool *	Yes, up to 25 days after permanent deletion (admin only)	No. After confirming, all calendar and events are immediately deleted cannot be recovered.	No. After 30 days, contacts are permanently deleted and cannot be recovered.

*Will not restore sent folder or discarded drafts

**Starting Oct 13th 2020, Google Drive trash items will be [automatically deleted after 30 days](#)



Microsoft 365

What happens to your files **after they're deleted?**

	Outlook	OneDrive	Outlook Calendar	Outlook Contacts
Kept in Trash	14 days*	30 days	No	14 days
Permanently Deleted from Trash	30 days	30 days	N/A	30 days
Restore After Deletion?	No	No (for non-365, work or school accounts)	No. After confirming, all calendar and events are immediately deleted cannot be recovered.	No. After 30 days, contacts are permanently deleted and cannot be recovered.

*Exchange Online administrators can change this setting to increase the “Retention Period” of deleted emails.




Be sure to use Microsoft Office version history!


Use Version History to view previous versions of files and restore them.

- *Office for Windows (Office 2016)*
- *Office 365*
- *Office for Mac, iOS, and Office Online.*


Version History

Today, September 15, 2020

 Modified by: Nichole Kucher 11:18 AM


 Modified by: Nichole Kucher 8:51 AM

[Open Version](#)


 Modified by: Guest Contributor 7:38 AM

[Open Version](#)


Yesterday, September 14, 2020

 Modified by: Nichole Kucher, Benny Kuo and Guest Contributor 4:33 PM


[Open Version](#)

 Modified by: Nichole Kucher 4:25 PM

[Open Version](#)

 Modified by: Nichole Kucher 4:12 PM

[Open Version](#)

ioSafe

Where to find version history



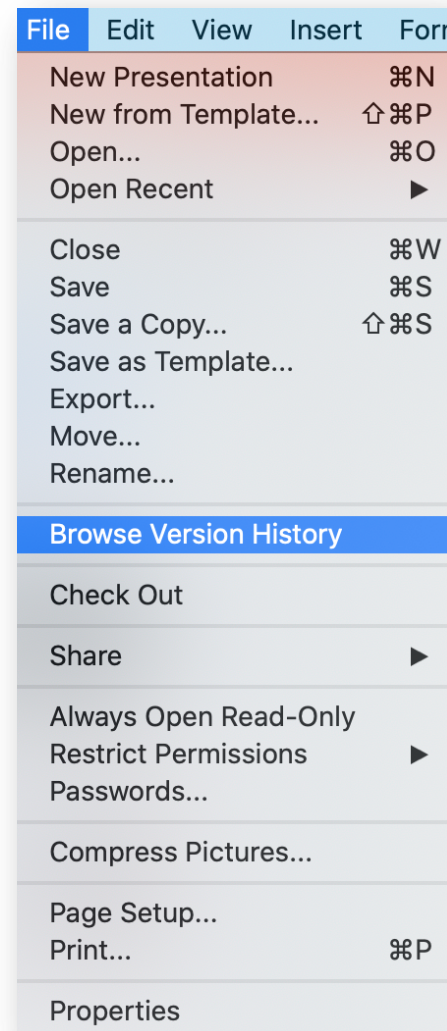
Windows

File > History > View and Restore Previous Versions



Mac

File > History > Browse Version History



Microsoft OneDrive

What happens to your files **after they're deleted?**

User Type	Kept in Recycle Bin	Kept in Second-stage Recycle Bin	Deleted from Second-stage Recycle Bin	Maximum Time Allowed to Restore Deleted Files
All users	30 days	30 days	Deleted forever	60 days
Office 365 users	30 days	30 days	Available for 30 days in "Settings"	90 days
Business/School user accounts	93 days	N/A	Within 14 days after 93 day period. Admins can contact Microsoft Support to request restoration, but this isn't guaranteed.	107 days

Second-stage Recycle Bin

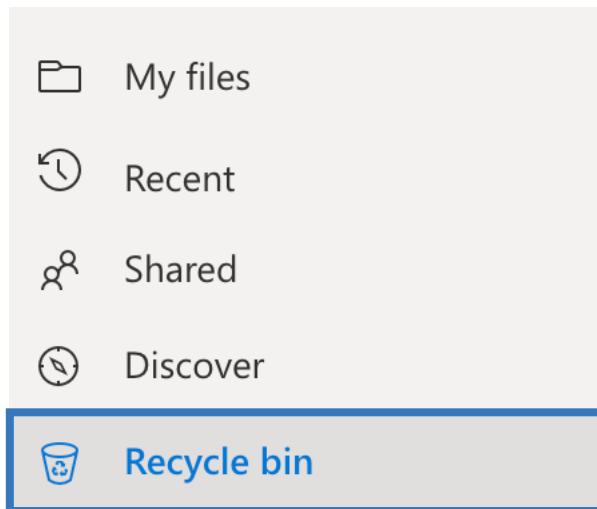
The second level of recycling for files that get deleted or moved from the regular recycling bin.

- **For Office 365 users and non-business/school accounts:**
 - After you've deleted a file and the first 30 day timeframe has passed, your files move into the second-stage recycle bin.
- **For business/school accounts:**
 - Your files move there after emptying the Recycle Bin.
 - Your files stay there for the remainder of the 93 day retention, or until a user permanently deletes the file.



View Your Second-Stage Recycle Bin

To access your second-stage recycle bin, go to your OneDrive file dashboard and select **Recycle Bin** in the left sidebar:



Then scroll down to the bottom of your Recycle Bin and click **Second-stage recycle bin**:

Can't find what you're looking for? Check the [Second-stage recycle bin](#)



OneDrive File Restore Limitations

If a major data loss incident happens, you can restore files to any point over the past 30 days using **OneDrive's Files Restore** feature.

However, one minor change or incident can make the **Files Restore feature fail**.

This could happen when:

- File restore versioning is turned off
- Site Collection Recycle Bin is emptied
- A file or folder is uploaded after deleting it (Files Restore will skip the restore operation for that file or folder)
- Ransomware encryption causes missing version history

Cloud data recovery
has an expiration date



A stylized graphic on the left side of the slide. It features a large, orange-red flame-like shape with three main peaks. Inside the lower-left portion of this flame shape is a smaller, light blue teardrop-shaped element.

How to extend the lifetime of your cloud-stored data

Hard drive failure happens

45%

of all backup failures
are hard drive failures

50%

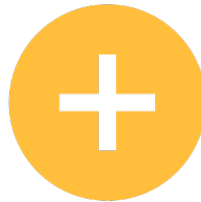
of backup restores fail

25%

of data loss is human error

Cloud or local backup?

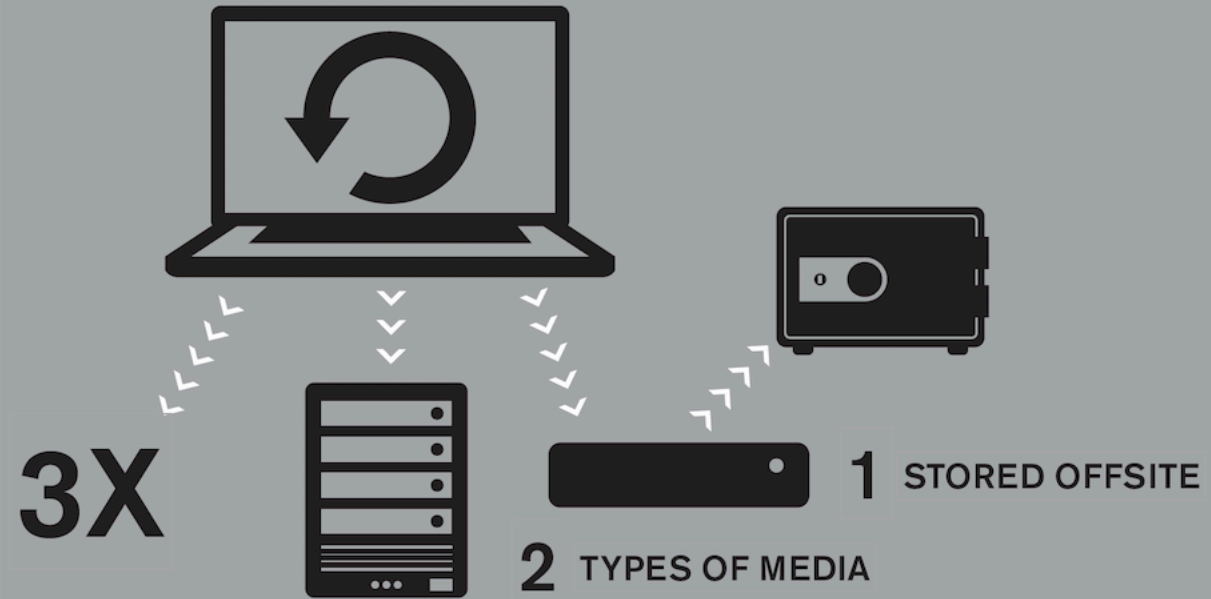
Both! A combination of local backup + cloud storage will make sure your files aren't lost



3, 2, 1, Backup!

Protecting and securing your files is as simple as following the **3-2-1 backup rule**.

- Make **3** copies of your important data
- on **2** different types of media (hard disk, SSD, thumb drives, DVD, or Bluray disks)
- with **1** of those backups stored at a different location





Design a backup plan that fits you

Local backup + disaster-proof storage + cloud storage can go a long way to securing your data and protecting your privacy.

Final Takeaways

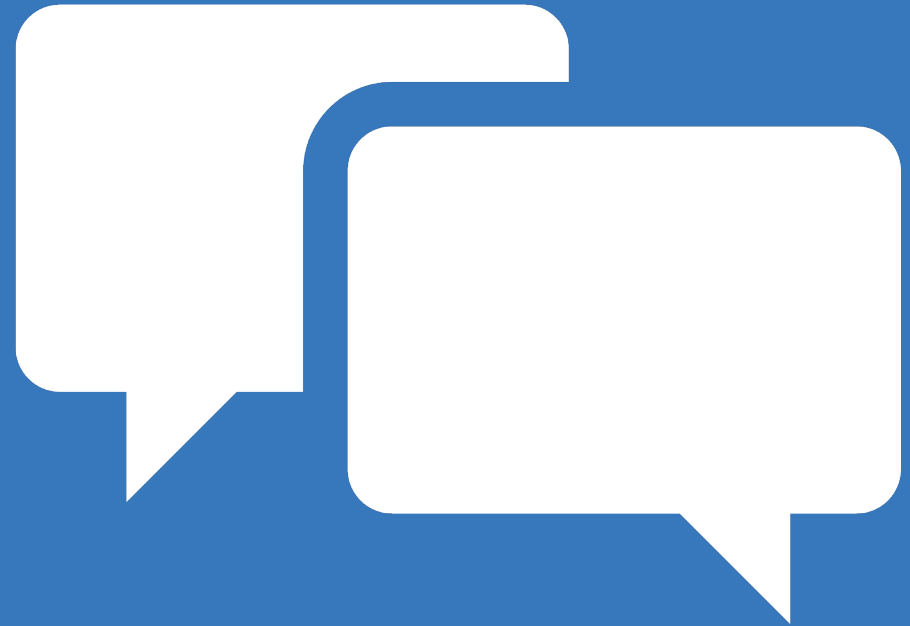
- The cloud is not a mythical creature – it's made up of physical devices controlled by humans.
- Weigh the advantages & disadvantages you might face with the cloud so your expectations are set correctly.
- The cloud is not infallible, and when possible, use a combination of local + cloud storage to back up your files.

Two copies are better than one

For an extra layer of security, create two redundant copies of your data simultaneously to eliminate the risk of data loss from drive failure.



Q&A



Thank you!

Contact ioSafe

+1 (530) 820-3090

sales@iosafe.com

Contact Leif

lwatkins@iosafe.com

Contact Nichole

nkucher@cdsg.com

ioSafe Headquarters

10600 Industrial Ave,
Suite 120
Roseville, CA 95678

Connect with us

 [iosafe](https://www.facebook.com/iosafe)

 [@iosafe](https://twitter.com/iosafe)

 [iosafe](https://www.linkedin.com/company/iosafe)

