Drive alternatives

Google Drive alternatives: Best picks

Google Drive is free and convenient, but it doesn’t care about your privacy. It scans and analyzes your data and retains the right to do whatever it wants with it. However, there are secure cloud drives that protect your business contracts, budgets and personal journals. No one should be able to view your private files unless you want them to. To ensure that only you can access your files on a cloud storage service, use an alternative.

Contents

- Why should you look for Google Drive alternatives?
    - Dropbox
    - Tresorit
    - pCloud

- Box
- Mega
- Sync.com
- SpiderOak One Backup

Why should you look for Google Drive alternatives?

It isn't the best option for people who care about their privacy and here's why:

1. Google scans and analyzes your data

Google admits to scanning all the documents you upload on your Drive. Any information collected about you is used to create your 'user profile' and show you personalised Google search results or Google ads. Some files you store on Google Drive might be very personal. Would you like such sensitive information to influence what's served to you online and be made public?

The company says that it scans and analyzes your files to improve their services and provide you with "personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection." However, it appears that Google bots that crawl your documentshave been trained to look for 'objectionable' content and then delete it without further explanation. What if a project you've been working on for months is suddenly irretrievably deleted?

Although Google encrypts your files, they are still not completely private. In their privacy statement, they admit that your documents could be accessed by Google in special circumstances, for example, if required by law enforcement agencies.

2. Google can manipulate your documents

Google's privacy agreement also states that they have a worldwide license to "use, host, store, reproduce, modify, create derivative works […], communicate, publish, publicly perform, publicly display and distribute" your documents uploaded on Google Drive.

They also state that, by using Google services, you agree to share your data with unspecified third parties that "Google works with." Such vague statements leave a lot of freedom for interpretation and show that what's stored on Google Drive is essentially Google's property.

RELATED ARTICLES

The best Gmail alternatives that you can really trustIn Depth · 7 min read
The complete guide to deleting your Google historyHow-To · 4 min read

---

3. You have little control over files you shared with others

Google allows you to quickly give viewing, editing or commenting permissions to your friends and colleagues. However, that presents even more privacy risks because these documents lack some basic security measures. It's difficult to track what happens with your shared documents as anyone with editing permissions can easily share the document with anyone else.

You can amend sharing permissions by going to advanced settings. However, you won't be notified if someone has shared your document, so you will have to keep an eye on who currently has access to it. What's even worse is that if you make your documents public, anyone will be able to find them

by simply using Google search.

4. Google Drive is more vulnerable than other cloud service providers

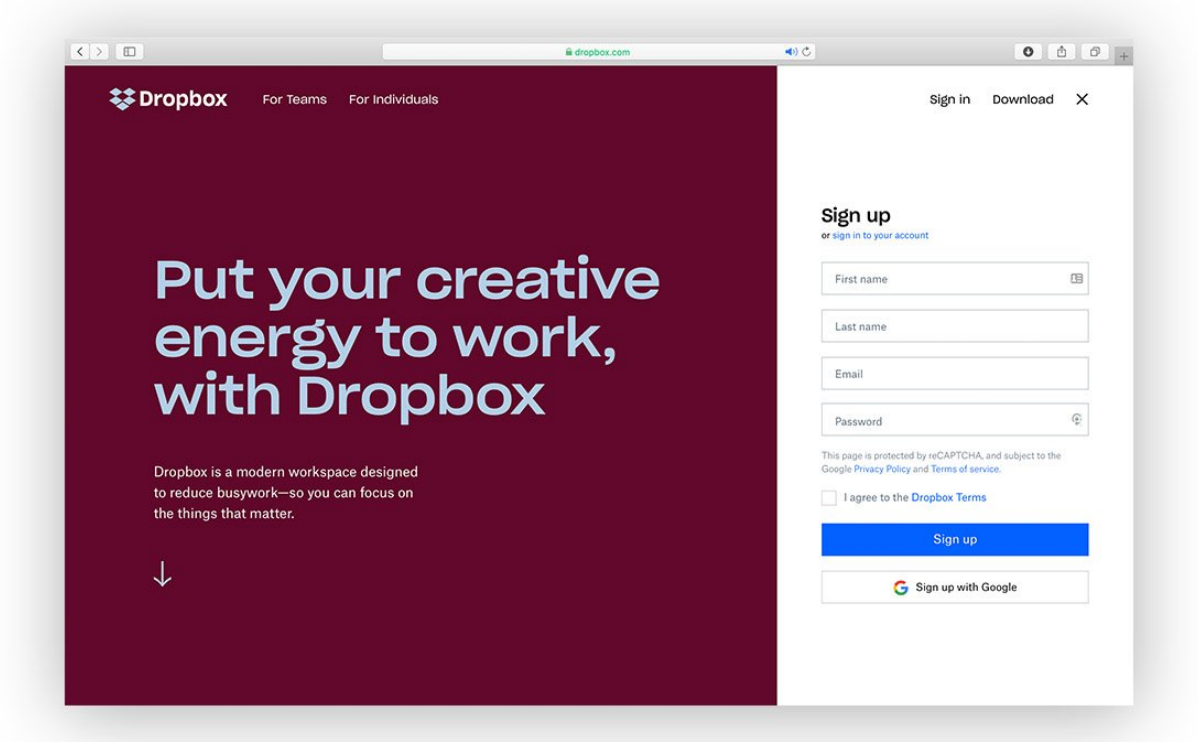
Google Drive is linked to your Gmail account, which means that if you forget to sign out of your account on a public computer or your account gets hacked, your Google Drive will be easily accessible too. There’s a saying that applies – don’t put all of your eggs in one basket.

There are so many Google Drive users that they’ve become targets for social engineering attacks. Phishing emails can masquerade as Google Drive or Gmail notifications and trick people into giving out their login details. If you care about your data, it’s time to choose a privacy-oriented cloud storage provider.

All apps featured in this post offer end-to-end encryption, but not all of them have zero-knowledge policies. When companies without zero-knowledge policies encrypt your files, they still hold the decryption keys and can read your files. Those with zero-knowledge policies cannot decrypt your documents as you’re the only one who has the key. If you lose it, your files will be lost too.

Dropbox

(Android, iOS, macOs, Windows, and even Linux)



Dropbox, the pioneer of cloud storage, invented block-level file transfer algorithms, which are now widely used by other cloud storage apps. With Dropbox, you can have a local folder on your computer, which automatically syncs all your files to the cloud, or you can simply use it online. The first time you upload something, it will transfer the whole file, but later, only the edits will be synced.

Dropbox is a great competitor to Google Drive. It’s easy to use, encrypts your data in transit and at rest, and offers two-factor authentication. It also has much stricter rules on who can share and edit your documents. However, only Dropbox Professional or Business customers can use extra features like link sharing, manual sharing permission changes, or remote file wiping. It’s also good to know that Dropbox runs on open-source software, meaning that anyone can look for vulnerabilities in its code.

However, there are still a few things Dropbox could work on:

- Teams that use Dropbox for business can all see, edit and share each other’s documents. Great for collaboration but not so great for privacy.

- Dropbox claims that they take their security seriously and they would never snoop on your files, unless, of course, required by law enforcement agencies.
- They don’t scan any uploaded documents for viruses or malware, meaning that any other devices linked to your account could be infected if you open a malicious file. However, this also probably means that your files won’t be scanned by bots and will remain private.

Tresorit

(Windows, macOS, Linux, Android, and iOS)

Tresorit is probably one of the safest and most private cloud drive service providers on the market. Its main features are its military-grade encryption and public key cryptography. This means that your files are encrypted before they leave the device and no one, not even Tresorit employees, can read the data stored on their servers. Tresorit trusts their encryption so much that it has offered $50,000 to anyone able to break it. According to them, more than 1,000 hackers, including

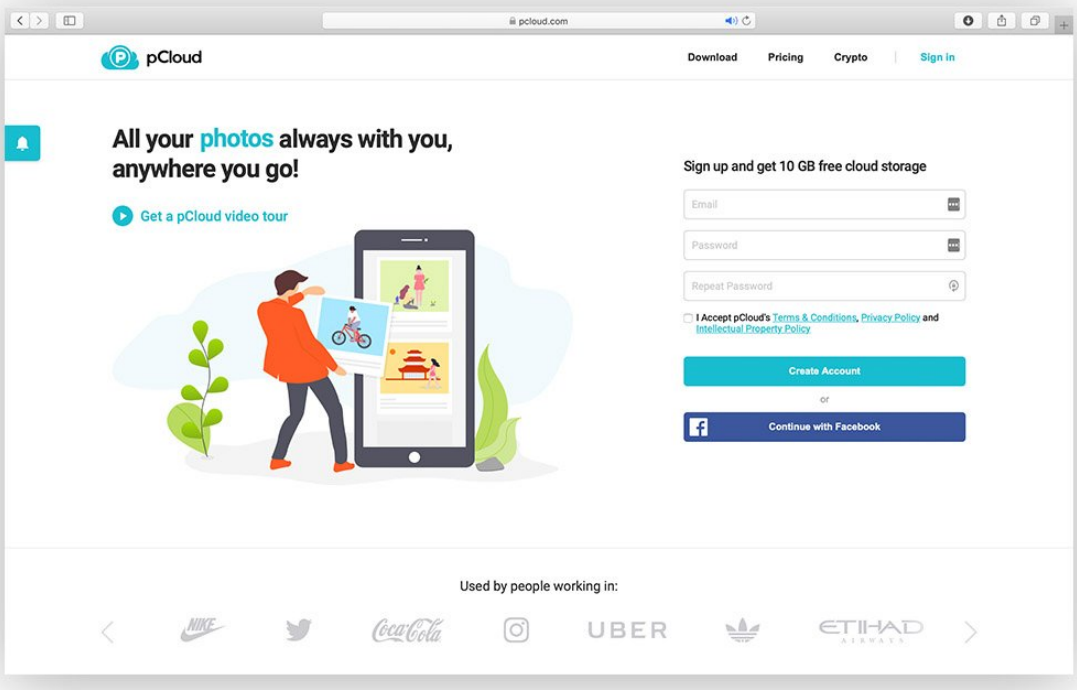
people from MIT, Stanford, and Harvard, have tried and failed.

Tresorit's file sharing security measures are significant. You can share files as you would on Google Drive, but it's much harder for someone else to transfer the ownership of your data. When you share a link to a file on Tresorit's server, a secret key is generated for that person exclusively. You can also check when and who downloaded the file you shared. If you're worried that the file might have leaked to someone else, you can immediately revoke access.

Tresorit's data centers are based in Europe, and the company falls under Swiss jurisdiction, so they have to comply with GDPR rules and regulations. This makes less likely that anything will be done with your data without your consent.

pCloud

(Android, iOS, Windows, macOS, and Linux)



If Tresorit focuses more on businesses, then pCloud is the perfect alternative for individuals. It offers an easy to use

software with encryption as strong as Tresorit’s. Unfortunately, the encryption service, called pCloud Crypto, is hidden behind a paywall. The app providers trust that it’s unbreakable and have offered $100,000 to anyone who manages to decrypt it. They even have a count of how many people have tried it so far – as of now, almost 3,000 hackers have tried and failed.

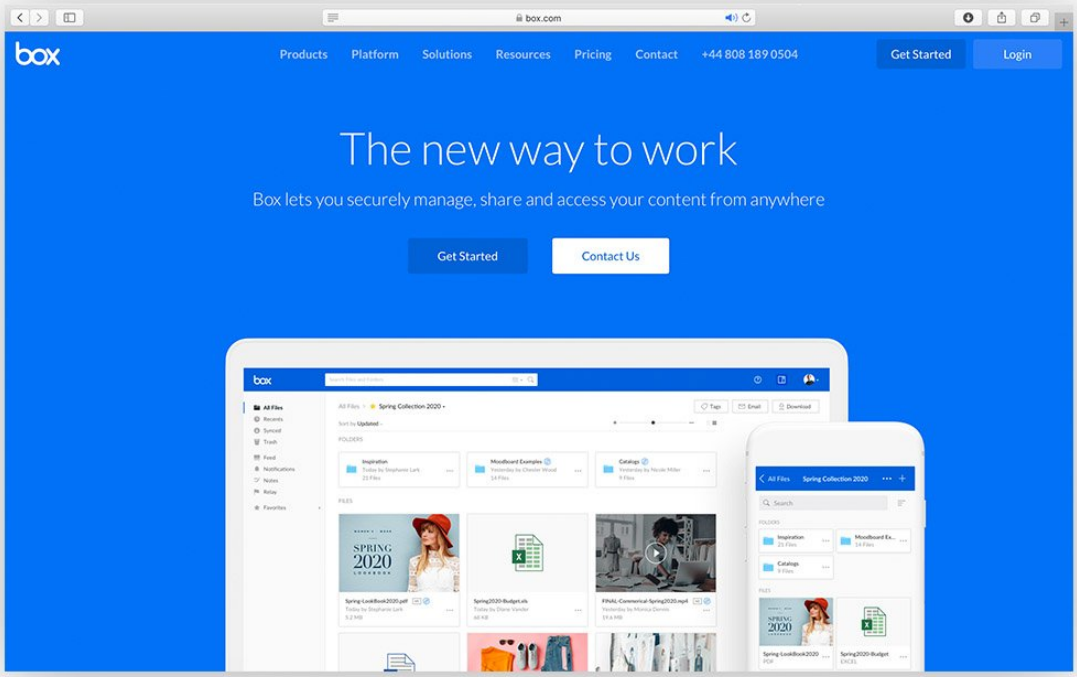
They are also serious when they say they care about your privacy. They have a zero-knowledge-protection policy, which means your files are encrypted before they leave your device. No one except you will ever be able to decrypt them.

If you need to share files with your team members or clients, you might want to consider pCloud Business. It will allow you to set up folders that you can share with your colleagues. The whole team can have the same editing permissions, or you can set them individually. It’s great for collaboration too, as it lets team members view a detailed log of edits and comment on shared files. If needed, you can even restore previous sessions for up to 180 days.

Another interesting thing about pCloud is that it’s the only provider that offers a one-off lifetime subscription. Unfortunately, if you wish to use pCloud Crypto, you will still have to pay extra on a monthly or yearly basis.

Box

(Android, iOS, Windows, and macOS)



The Box is an excellent alternative for businesses and small teams. It offers a secure storage platform, lets you choose where your data will be stored, and gives you a plethora of collaboration tools.

With Box, you can create files that will instantly be shared with your teammates. They can then edit and comment on your documents in real time. The Box is probably one of the most integrated apps on this list, too. With over 1,000 leading software providers like Office 365, Salesforce and Adobe Sign, your teammates will be able to edit documents without leaving the platform. It also gives you detailed version tracking so you can see every sync and change ever made.

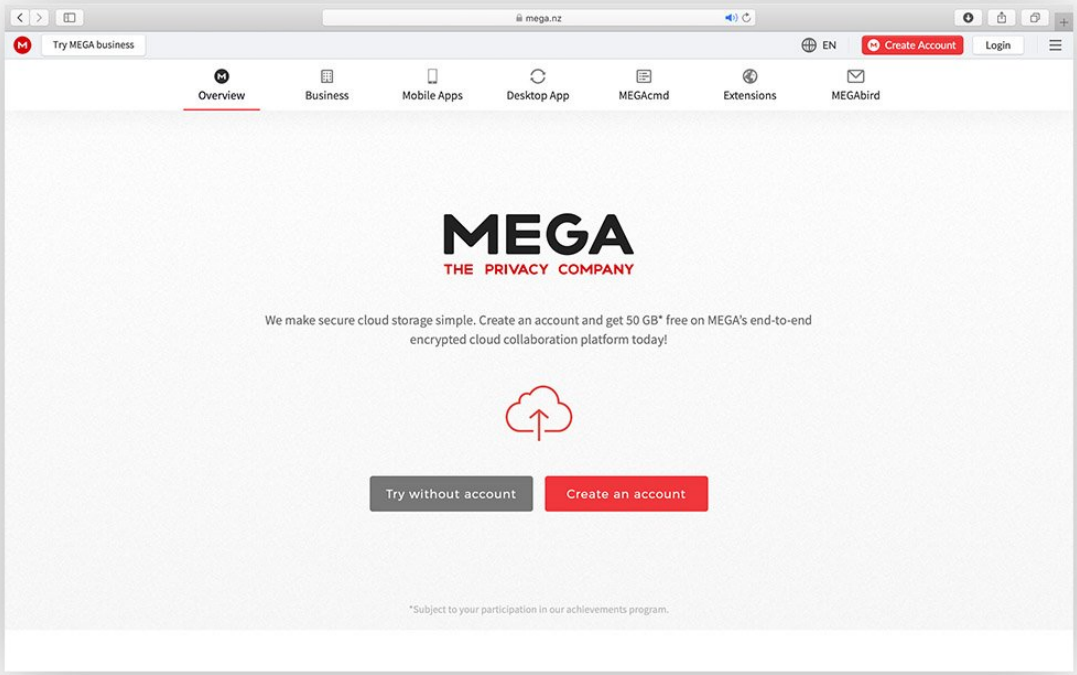
If you wish to share a file externally, you can do so by sending a link or creating a custom URL. As such links can still raise security concerns, Box allows you to set passwords on shared files too. If you accidentally send it to the wrong person, change their permission settings or simply revoke access.

What makes Box really stand out from its competitors is the use of machine learning. It makes workflows a breeze – tasks

assignment, deadline setting and progress tracking – all can be done in Box. It will even help you automate tasks, direct them to the right people and generate new contracts. However, this feature raises some privacy concern. The company doesn't identify how the software collects and analyzes this information.

Mega

(Android, iOS, Windows, macOS, and Linux)



Mega is probably the best option if you are looking for a free and secure service with a lot of storage. It encrypts your data in transit and at rest, offers collaboration tools and lets you share your files. It's also the only cloud storage service that offers you a generous 50GB completely free. You can add even more storage if you invite your friends or download their mobile app. However, Mega has some limitations:

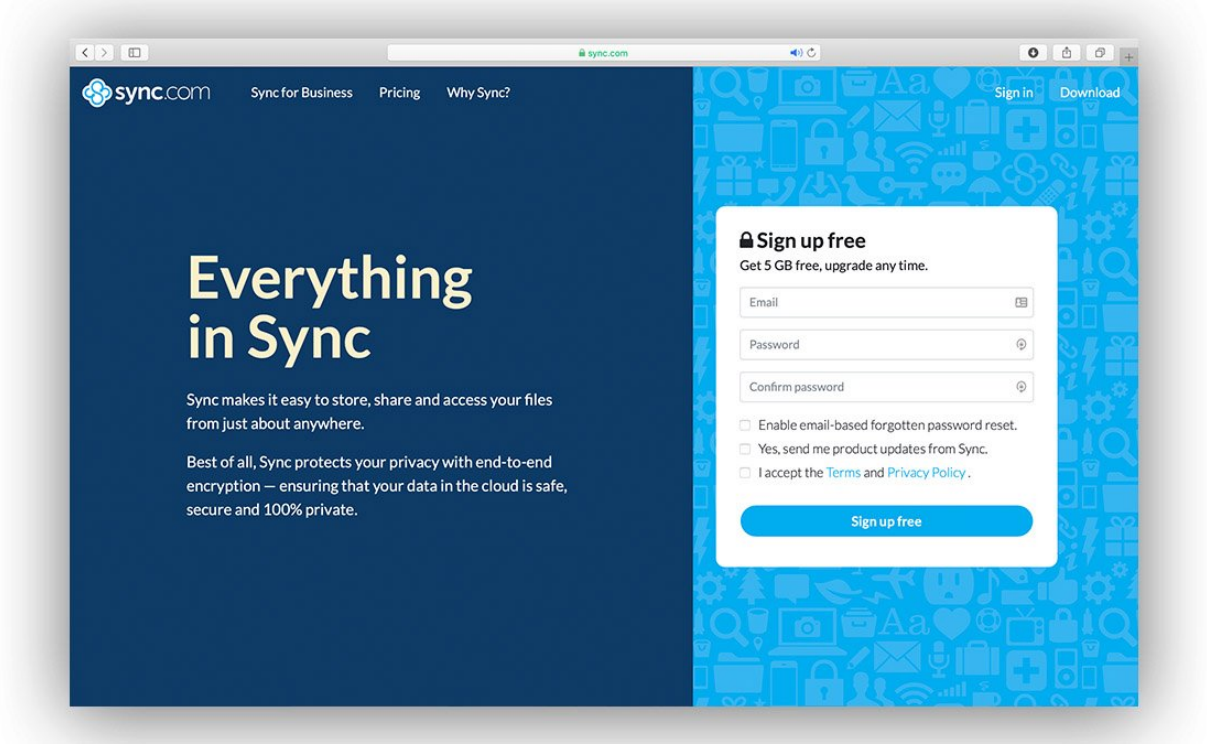
- Collaboration tools are great as they let you see edits in real time, but they are nowhere near as advanced as Box's.

- You can share files by sending a link, but it doesn't have any extra security features like password protection.
- It has a bandwidth limitation of 10GB, which refreshes every 30 min. This might be bothersome for those who want to transfer huge amounts of data. Other providers offer unlimited bandwidth.

Even though Mega's headquarters are in New Zealand, the company complies with GDPR rules. It's also great that Mega was built on public source code, so anyone can have a peak and look for its vulnerabilities.

Sync.com

(Android, iOS, Windows, and macOS)



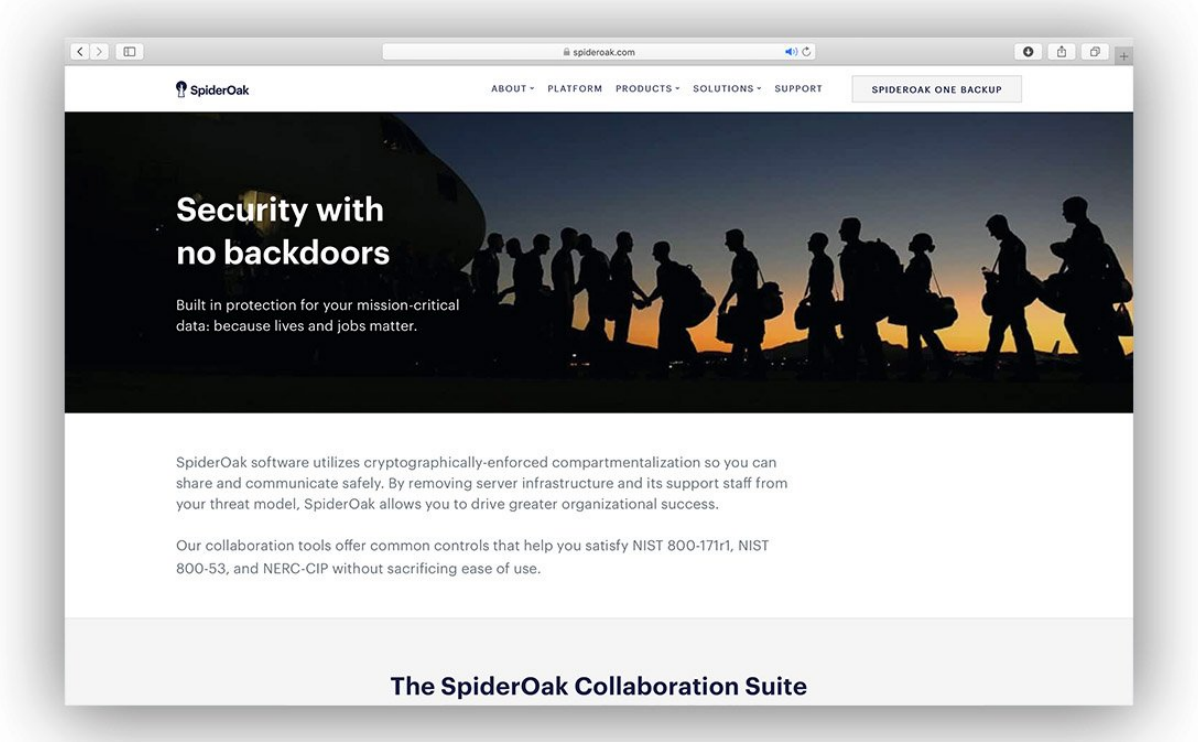
If you are looking for functionality similar to Dropbox, highly secure encryption like Tresorit, and a lot of storage, Sync.com is your best bet. This cloud storage provider places a folder in your device and uploads any documents you add to it to the cloud. All your files can then be synced over

multiple devices. It also offers end-to-end encryption and zero-knowledge policy, so no one, not even Sync employees, will be able to see your files. You can store up to 2TB of data for only $8 a month.

You can also share files and entire folders with others and protect them with passwords. You can decide on the level of access you want to give them, set permission expiry dates, or simply revoke them at any time. Sync.com also allows you to remotely disconnect your devices in case they've been lost or stolen.

SpiderOak One Backup

(Android, iOS, Windows, macOS, and Linux)



SpiderOak is yet another product that offers strong end-to-end encryption and a zero-knowledge policy. So any documents backed up on SpiderOak servers will not be seen by its employees or anyone trying to intercept it. (Though be aware that this cloud storage provider is based in the US and doesn't comply with GDPR rules as its European counterparts.)

Unfortunately, strong encryption might be the only significant feature SpiderOak has to offer. Its interface is harder to use than Google Drive or Dropbox, and it doesn’t have team collaboration embedded in the app. Instead, SpiderOak designed two more, completely separate products – SpiderOak Share and SpiderOak Semaphor messaging. The former provides encrypted document sharing and collaboration while the later is a secure messaging app. It’s surprising that they opted for such a solution as other providers have all these features integrated into one platform.

References

- https://nordvpn.com/blog/google-drive-alternatives/