

Forum:[Hack Forums](#)

Thread: [Cloud storage? Dropbox, OneDrive, Google Drive?](#)

gurlhackerclub - April 17, 2020, 4:24 am

Cloud storage? Dropbox, OneDrive, Google Drive, Mega?

Marxist - April 17, 2020, 4:27 am

What's your question?

If you're asking what I use I don't use any of them. I host my own Nextcloud instance on a shitty server at my house, and route the traffic through a VPN I own.

Not very exciting. But keeps my data physically in my control.

Spoiler ([Click to View](#))

humanbody - April 17, 2020, 4:29 am

I use Google Drive as I've been using it since the beginning and I am kinda used to it, I have set it up so it automatically updates as soon as I copy & paste & modify a file and I can use it on mobile as well. But if there are other better alternatives that I don't have to go through 100 steps in order to access my files then I will be more than happy to switch.

shitmaster - April 17, 2020, 4:30 am

None of the above. Maybe a home cloud solution. I mean at least I have a home cloud solution and I feel safer with regards to privacy.

Exposed74 - April 17, 2020, 4:32 am

(Apr 17, 2020 04:24 AM)gurlhackerclub Wrote: [\[CITE\]](#) Cloud storage? Dropbox, OneDrive, Google Drive, Mega?

Words ? Verb ? Sentence ?

gurlhackerclub - April 17, 2020, 4:57 am

(Apr 17, 2020 04:27 AM)Marxist Wrote: [\[CITE\]](#) What's your question?

If you're asking what I use I don't use any of them. I host my own Nextcloud instance on a shitty server at my house, and route the traffic through a VPN I own.

Not very exciting. But keeps my data physically in my control.

Spoiler ([Click to View](#))

Good idea running through a VPN. I used to have a Nextcloud instance running on a Pi, Then port forward from my router. But seeing so many vulns pop up on hackerone, Maybe not safe to be open to the net yet.

Marxist - April 17, 2020, 5:03 am

(Apr 17, 2020 04:57 AM)gurlhackerclub Wrote: [\[CITE\]](#) Good idea running through a VPN. I used to have a Nextcloud instance running on a Pi, Then port forward from my router. But seeing so many

vulns pop up on hackerone, Maybe not safe to be open to the net yet.

The VPN thing is easy, you just forward your desired ports through the VPN. Or don't and keep it all internal to the VPN, so people outside of the VPN can't access it. Only downside is your devices must connect to the VPN to access it. Which is hectic with mobile devices. However, it ensures all your data is encrypted Point-to-Point from device and server, Which is then encrypted at rest on the server.

My whole home set up is basically an enterprise solution ???

And meh, I haven't seen much on the new update. Everything you use is going to have vulns, you just have to keep an eye out and try and mitigate risk.

Shitty example of forwarding through a VPN

```
Code iptables -A FORWARD -i eth0 -o tun0 -p tcp --syn --dport 443 -m conntrack --ctstate NEW -j ACCEPT
```

```
iptables -A FORWARD -i eth0 -o tun0 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A FORWARD -i tun0 -o eth0 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to-destination 10.8.0.100
```

```
iptables -t nat -A POSTROUTING -o tun0 -p tcp --dport 443 -d 10.8.0.100 -j SNAT --to-source 10.8.0.1
```

```
iptables -A FORWARD -i eth0 -o tun0 -p udp --dport 443 -m conntrack --ctstate NEW -j ACCEPT
```

```
iptables -t nat -A PREROUTING -i eth0 -p udp --dport 443 -j DNAT --to-destination 10.8.0.100
```

```
iptables -t nat -A POSTROUTING -o tun0 -p udp --dport 443 -d 10.8.0.100 -j SNAT --to-source 10.8.0.1
```

SIM-3257834 - April 17, 2020, 5:05 am

I'd just go the next cloud route under a VPN. Fuck Google Google services and Microsoft.

4dik - April 17, 2020, 5:06 am

I don't use any of these I have my own personal backup server in my home! More secure and safe

Weddy - April 17, 2020, 5:10 am

Server at home is the best.

I would never trust Google or Microsoft as said above.

Luca - April 17, 2020, 5:11 am

I use Google Drive and OneDrive.

Yanix - April 17, 2020, 5:48 am

(Apr 17, 2020 05:06 AM)4dik Wrote: [\[CITE\]](#) I don't use any of these I have my own personal backup server in my home! More secure and safe

This is what I am thinking that's why I am not using any of these...files are not secure and safe.

4dik - April 17, 2020, 5:49 am

(Apr 17, 2020 05:48 AM)Yanix26 Wrote: [\[CITE\]](#) This is what I am thinking that's why I am not using any of these...files are not secure and safe.

Yeah Im not the biggest fan of anyone! my backup is an actual offline back up, so know can get access to it unless they get access to it

Yanix - April 17, 2020, 5:52 am

(Apr 17, 2020 05:49 AM)4dik Wrote: [\[CITE\]](#) Yeah Im not the biggest fan of anyone! my backup is an

actual offline back up, so now can get access to it unless they get access to it
It's better to be keeping your files safe than sorry later ???

Yin Yang - April 17, 2020, 6:03 am

I've been using google drive since I primarily use my gmail account

Scooby - April 17, 2020, 6:44 am

I use Google drive for anything I don't mind the government seeing. Anything else is kept offline or encrypted before being put in my Google drive.

Bastille - April 18, 2020, 1:43 am

One Drive most of the time, mainly for work.

Google drive for huge files I just need to transfer from a computer to a remote one, and then I delete it.

tdbnz123 - April 20, 2020, 7:36 pm

Tresorit

– A premium secure cloud storage solution in Switzerland

+ Pros

End-to-end encrypted with AES-256, TLS

Based in Switzerland, a privacy-friendly jurisdiction

GDPR compliant

Supports 2FA

3 GB storage (free plan); 200 GB – 2,000 GB (paid plans)

24/7 support

Telephone, email, live chat support

- Cons

Paid versions are expensive

Not open source

Complicated to use

Tresorit feature summary

Here is a quick summary of the major features of Tresorit, which we'll cover more below. Note that some of these features are only available in one or more of the paid Tresorit plans.

Supported platforms include Windows, Mac OS, Linux, Android, iOS, major web browsers

End-to-end data encryption using AES-256 and TLS

Massive amounts of file storage

Fine control of synchronization with deleted version recovery

Synchronizes across all your devices and browsers

Administrative reports & analysis

Third-party security tested with numerous industry certifications

Plans for every level of user from individual to enterprise

2FA support

Where does Tresorit store user data?

By default, the data you store in Tresorit is encrypted and stored in data centers in Ireland.

However, business and enterprise customers can opt to store their data in the US (East and West coast), the UK, Canada, Ireland, Germany, Switzerland and France.

MEGA cloud – A secure and private cloud storage with a free tier (based in New Zealand)

+ Pros

End-to-end encrypted with AES-128, TLS

GDPR compliant for all users worldwide

Supports 2FA

Free and paid plans

No data stored in United States

Transparent source code

Massive amounts of storage available

File versioning

Annual transparency reports

– Cons

Not open source

Confusing free plan

No live chat or phone support

No published third-party audits or testing

MEGA feature summary

Here is a quick summary of the major features of MEGA. Note that some of these features are only available to users with PRO or Business accounts.

Supported platforms include Mac, Windows, and Linux desktops

Android, iOS, Chrome, Firefox, and Opera browser extensions

End-to-end data encryption using AES-128 and TLS

Storage ranging from 15GB to 16TB

Synchronizes across all your devices and browsers

Administrative reports & analysis

2FA support

File versioning

Company information

MEGA was launched in 2013 in New Zealand by Kim Dotcom. Mr. Dotcom severed all ties with MEGA in 2015, but the company has continued to grow and thrive. At the time of this review, the service has over 166 million registered users worldwide.

Company information

MEGA was launched in 2013 in New Zealand by Kim Dotcom. Mr. Dotcom severed all ties with MEGA in 2015, but the company has continued to grow and thrive. At the time of this review, the service has over 166 million registered users worldwide.

Sync.com -- A good cloud storage provider in Canada.

Sync.com is one of the leading secure cloud storage services. It offers excellent security and

privacy with its end-to-end (zero knowledge) encrypted network, along with large amounts of storage and bandwidth. At the same time, it has some limitations that may make it unsuitable for certain applications.

We'll look at both the good and the bad in this Sync.com review, with the aim of helping you decide whether this could be your future cloud storage solution.

+ Pros

- End-to-end encrypted with AES-256, RSA-2048, and TLS
- HIPPA, GDPR, PIPEDA compliant
- Supports 2FA
- 5 GB storage (free plan); 200 GB – unlimited (paid plans)
- Unlimited version tacking and restoration
- Unlimited file sizes
- Unlimited upload/download quota

– Cons

- No Linux desktop client
- Limited sync folder options
- No monthly billing plans
- No integration with third-party products

Sync.com feature summary

Below is a quick summary of the major features of Sync.com. Note that some of these features are only available with paid plans.

Supported platforms include Windows, macOS, Android, iOS, major web browsers

End-to-end data encryption using AES-256, RSA-2048, and TLS

5 GB to unlimited amounts of file storage

Unlimited upload/download

Extensive options for controlling access to shared files

Ability to recover deleted files or roll back entire account

Synchronizes across all your devices and browsers

Plans for every level of user from individual to enterprise

2FA support

Vault for non-synched cloud storage

Company information

Sync.com, Inc. was founded in 2011 by the founders of the web hosting company Netfirms. Based in Canada, the company is 100% Canadian owned and operated. It is governed by Canadian laws, including PIPEDA, the Personal Information Protection and Electronic Documents Act. 2015 was the year when the company officially launched Sync.com desktop and mobile apps. According to their website, over 750,000 businesses and individuals use the service.

While Canada is a member of the Five Eyes Alliance (FVEY), its privacy protections are generally considered to be better than those of the United States. That said, many privacy advocates advise against using services based in FVEY countries.

Where sync.com data is stored

The servers where your data is stored are physically located in Toronto, Ontario, Canada. All data

is encrypted in transit and at rest. Since Sync.com does not have access to your encryption keys, they are unable to decrypt your data. The company further states,

Nextcloud – A popular, open-source solution for cloud storage.

Nextcloud is an incredibly flexible cloud storage system. You can configure it in many different ways, and integrate it with over one hundred third-party apps

+ Pros

- FOSS (Free Open Source Software)
- Self-hosted and third-party hosted data options
- HIPAA and GDPR compliant
- Supports 2FA
- Integrated personal information management
- Optional integration with third-party apps
- Optional version tracking
- Nextcloud Hub for in-house collaboration
- Regular and Enterprise version

– Cons

- End-to-end encryption not fully implemented yet
- Company-authorized, third-party scanning of your system

Nextcloud feature summary

Here is a quick summary of the core features of Nextcloud.

- FOSS that runs on Windows, Mac OS, Linux, Android, iOS, and major browsers
- Multiple data hosting options
- Data in transit protected with TLS
- Optional at rest encryption using AES-256
- Optional end-to-end encryption with AES-128-GCM (not yet fully implemented)
- Optional file versioning
- 2FA support
- File sharing with numerous control options
- Integrated Personal Information Management (calendar, contacts, notes, tasks)
- Media streaming
- Synchronizes across all your devices and browsers

Where does Nextcloud stores user data?

Obviously, your data is stored somewhere when you use Nextcloud. But I can't tell you where it will be stored. That's because Nextcloud works through partner hosting companies around the world. They are the ones who store your data, be they located in Germany, Switzerland, Kuala Lumpur, wherever. You can also self-host your data on any server you have access to anywhere in the world.

The Nextcloud approach to data storage is incredibly flexible. But it also puts the burden of deciding where your data should be stored on your shoulders. You'll want to choose a country for your data based on your threat model, your country of citizenship, and where you are going to be located when you access that data.

There you go there is some useful information for you

Enjoy

tdbnz123

techpacket - October 7, 2020, 1:46 am

For cloud storage Google drive is the leading, you can also can take dropbox but suggestion is to use GDrive.

ETH - October 7, 2020, 4:11 am

(Apr 17, 2020 05:48 AM)Yanix Wrote: [\[CITE\]](#) This is what I am thinking that's why I am not using any of these...files are not secure and safe.

(Apr 18, 2020 01:43 AM)Yseurk Wrote: [\[CITE\]](#) One Drive most of the time, mainly for work.

Google drive for huge files I just need to transfer from a computer to a remote one, and then I delete it.

My guys use this <https://cryptomator.org/> to encrypt and upload on drive as no one can decrypt that For others also use those !

I use disroot cloud services powered by the nextcloud and for college purposes they provide us google drive unlimited, i use for that

SIM-4807019 - October 7, 2020, 12:32 pm

(Apr 17, 2020 04:30 AM)shitmaster Wrote: [\[CITE\]](#) None of the above. Maybe a home cloud solution. I mean at least I have a home cloud solution and I feel safer with regards to privacy.What help home cloud gives if your backups are still stored in home? why not encrypt stuff and upload in google or other so no robber can steal your shit?

atsavurdu - December 19, 2020, 4:04 pm

(Oct 7, 2020 12:32 PM)Dr.cha0s Wrote: [\[CITE\]](#) What help home cloud gives if your backups are still stored in home? why not encrypt stuff and upload in google or other so no robber can steal your shit?

Correct. In my case, I setup a local cloud at a friend for his work documents, which backs up on a external hard drive too. I cut a big slice for my home computer stuff.

I use SeaFile, it is great and faster than nextclud

GroguMando - December 20, 2020, 8:14 am

I use Onedrive for personal files, and Googledrive for anything else I just need to move, or send

2xTheTap115 - December 21, 2020, 9:56 am

(Apr 17, 2020 04:24 AM)gurlhackerclub Wrote: [\[CITE\]](#) Cloud storage? Dropbox, OneDrive, Google Drive, Mega?

As for me MEGA, I have been using it for several years and I am satisfied (Pro Lite version) Additionally, it is quite safe

FeatherLive - December 24, 2020, 7:20 pm

Mega and Google drive are my personal favorites, although I sometimes use OneDrive

?Ñâzg?l - December 30, 2020, 12:43 am

use Backblaze it has the cheapest storage option (also first 50 GB is free)
and you have apps that you use to encrypt your data yourself

also mega has a open source client that encrypts data before leaving server and supports 15 GB of free data

Framework - December 30, 2020, 8:46 am

I would honestly suggest none of them.

It's hard to trust any companies in handling your data, they have their own little loopholes where they are legally allowed to do whatever they want with your data.

Jinu - December 30, 2020, 10:31 pm

I am using GoogleDrive. And I recommend using GoogleDrive it is very convenient and easy to use. Especially in the educational field.

ETH - December 31, 2020, 6:29 am

i created my selfhost cloud and with vpn only access powered by the nextcloud

Navos - January 9, 2021, 11:46 pm

Seen a few people hosting their own cloud here.
A really good idea to be in control of your own data.

Larry - January 10, 2021, 3:28 am

Nextcloud.

Host it yourself