ownCloud
STORE. SHARE. WORK.

Why you want ownCloud

Standalone or as second Strategic Filesharing Platform next to MS OneDrive

Goal
Corporates want to enable seamless collaboration and improve productivity while at the same time aiming to save money (reduce storage costs, reduce operational and labor costs).

Partial solution
Transfer of desktop applications into the cloud.
The most popular offering is Microsoft Office 365 which comes with OneDrive to store and share files.

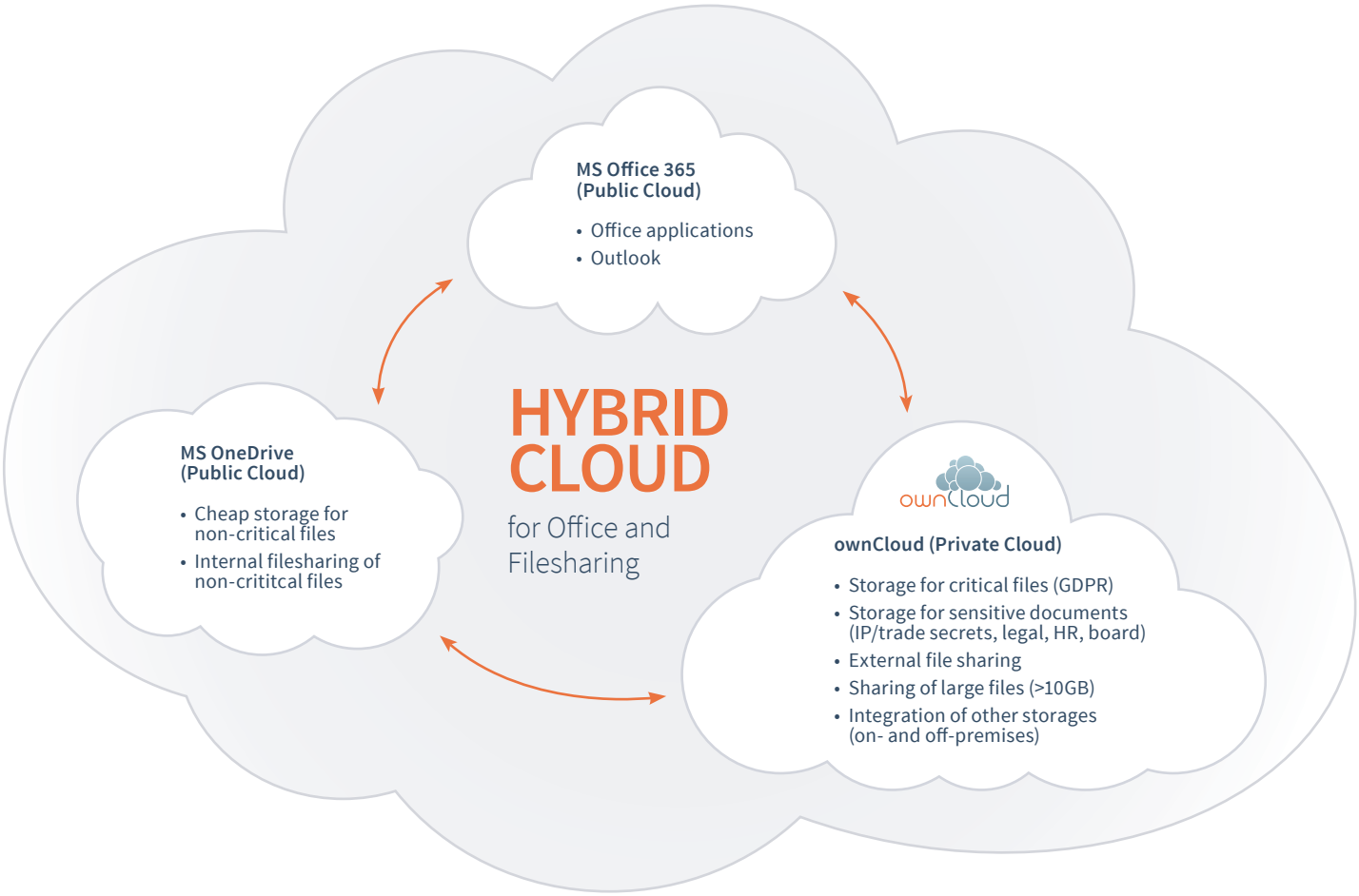
Fact
Based on the "Cloud Act" the US government can access all data stored in clouds of US vendors like Microsoft, Amazon, Google, Dropbox etc., no matter where the data center is located (in or outside of the USA). The Trump administration banned Google from working with Huawei and they could restrict access to data of European companies stored in clouds of US vendors in conjunction with prosecution or the smoldering trade conflict between the USA and Europe.

Challenge

1 Microsoft struggles with the EU GDPR as of 2018. According to an assessment of the dutch ministry of justice MS Office 365/OneDrive is not GDPR-compliant! https://www.rijksoverheid.nl/documenten/rapporten/2018/11/07/data-protection-impact-assessment-op-microsoft-office

Main reason: MS Office 365/OneDrive is nontransparent regarding the kind of data sent to Microsoft such that the admin/user cannot determine where and for how long sensitive data is stored.

Important: the recently introduced privacy dashboard (for Windows 10 only) does not eliminate the risk of being in breach of the GDPR as Microsoft regularly releases new functions in Office 365/OneDrive without prior notice and there's no possibility to prevent GDPR breaches by these new functions. So a system might be GDPR-compliant at a certain point in time and be in breach of the GDPR the next day.



State of the art Hybrid Cloud for Office and Filesharing- sensitive Files stay in Private Cloud

Furthermore one of the GDPR's core going-forward obligations is the duty to conduct Data Protection Impact Assessments (DPIAs) over processing activities that create a "high risk" to individuals' privacy (article 35). DPIAs constitute an important aspect of GDPR compliance. DPIAs are obligatory for all data contained in blacklists (please refer to annex) compiled by European Data Protection Authorities (DPAs). As a result of the 'cloud act' (https://owncloud.com/cloud-act-passed-by-us-congress/) which allows the US government to access all data stored in clouds of US-vendors like Microsoft independently from their storage location the result of all DPIAs must be negative. This means that all data contained in the blacklists of the DPAs cannot be stored in MS OneDrive. Prominent examples are personnel data, patient records and surveillance videos.

2 Due to the 'Cloud Act' sensitive information like intellectual property, trade secrets, legal documents and all kind of documents from board members should not be stored in an US-cloud like MS OneDrive. The US government can justify all data accesses just by using National Security! There's no controlling organ (like a judge) and they don't have to advise or disclose any data access. Since Snowden it's known that the US government is not reluctant re data access. Thanks to the 'cloud act' it's irrelevant which country the data is stored in.

3 Public cloud platforms like Microsoft Office 365/ OneDrive offer good integration between their own applications but naturally do have tight limitations when it comes to the integration of customer specific IT infrastructure. This results in a limitation of the use cases that can be covered with Microsoft Office 365/OneDrive. Every larger organization or company has filesharing use cases which can not be covered with MS OneDrive.

4 If you follow a one vendor strategy re file sharing and storage this results in a vendor lock-in. A vendor lock-in poses a risk for your organization.

Complete solution

ownCloud as either

(a) the secure on-premises file storage and sharing replacement for OneDrive or

(b) the second Strategic Filesharing Platform next to OneDrive to store all sensitive data, to cover all the use cases that can't be covered with a public cloud platform like OneDrive and to avoid a vendor lock-in.

ownCloud is your only or second strategic filesharing platform if you need to

1 store and share data contained in the blacklists of the DPAs

2 store and share sensitive data, which can't or shouldn't be accessible by the US government

3 comply with special data protection regulations

4 provide a solution for specific use cases that can't be covered with OneDrive or add filesharing functionality to other applications (i.e. filesharing within a supplier portal)

5 to securely share files (no public link) with external (partners) without provisioning them in your Active Directory/Domain

6 share large files (>10Gb) or large amounts of files

7 integrate infrastructure components (such as specific Authentication systems, Windows Network Drive, FTP-Server etc.)

8 provide easy-to-use end-to-end-encryption

9 operate the platform autonomously (independent of an internet connection)

10 be 100% sure that the software contains no „backdoors" and you need to be able to prove it

11 provide a branded filesharing platform (incl. clients/ apps)

12 solve your „Dropbox problem" (employees are using private Dropboxes to conveniently store and share company's documents with external people)

13 regularly share files with guests (full functionality but no quota) and you don't want to pay fully for these guests

14 conveniently collect data from multiple external parties (file drop)

15 migrate data from cloud storage services like Dropbox, box or Google Drive

16 implement a hybrid cloud strategy with sensitive (confidential) data remaining on-premises

17 a cost efficient filesharing solution for many internal end external users

18 share documents without download possibility (secure view with watermarks containing an identifier of the viewer)

19 be able to determine the lifetime of a file (i.e. for GDPR-compliance)

What neither Microsoft nor Google can offer is:

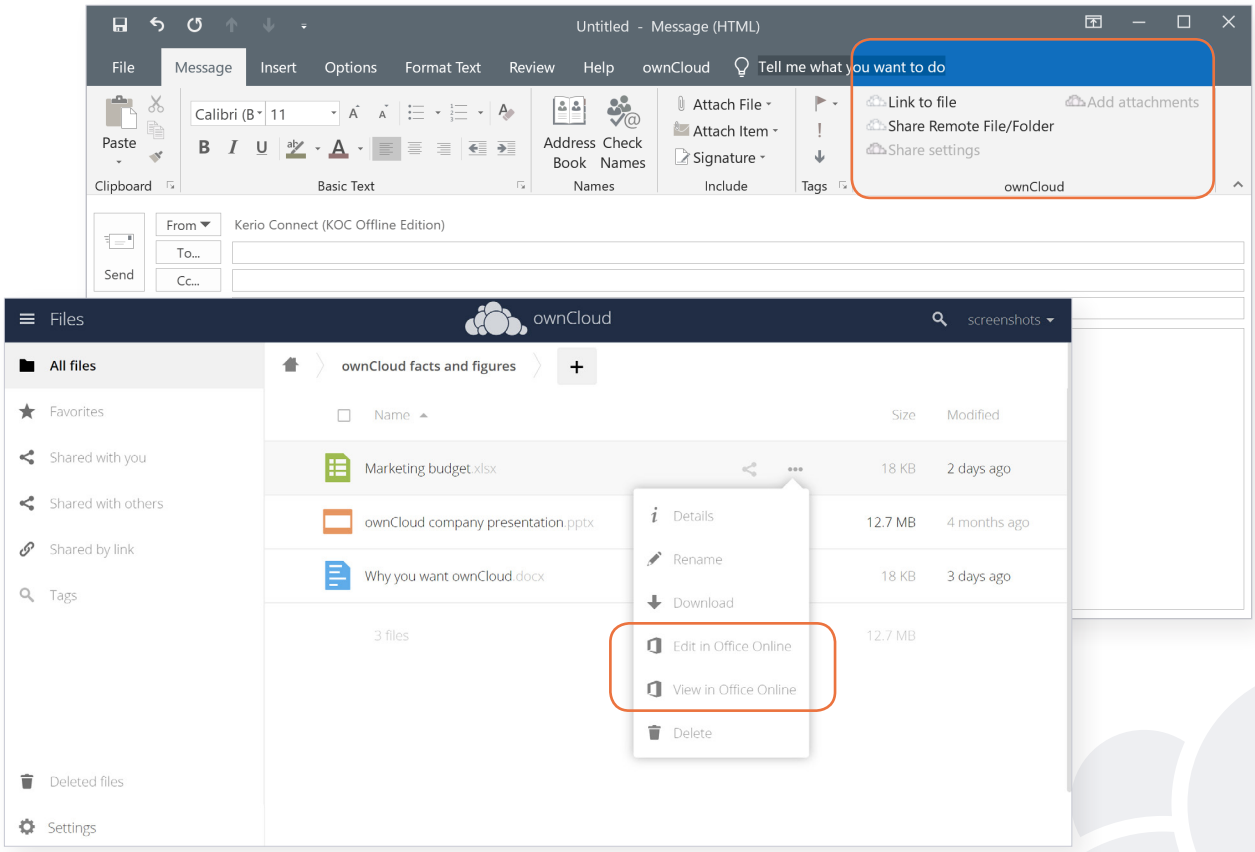
1. Unlimited file size
2. Branding
3. Flexibility/Integration
4. File access control
5. Secure view (protected with watermarks)
6. Open Source software (auditable)

Integration in MS Office/OneDrive:
ownCloud is perfectly integrated in MS Office 365 and OneDrive for a best possible user experience. For example users can:

- Access and share files stored in OneDrive via ownCloud
- Edit MS Office documents in ownCloud (also collaborative editing with MS Office Online Server)
- Share folders and files directly from MS Outlook (via Outlook-Plugin)

Freedom of Choice / Future Proof:
ownCloud is the only vendor that give customers the freedom of choice where and how to deploy:

- 100% on premise
- 100% at your personal hosting partner
- 100% in the Public Cloud (Amazon, Azure, …)
- Hybrid: ownCloud Management in your protected environment and encrypted data in the public cloud: be in control of your meta-data, keys, encryption algorithms, etc. while at the same time profit from cheep storage in the public cloud.



Summary

- With ownCloud you can cover current and future requirements that cannot be covered with MS OneDrive.
- ownCloud is perfectly integrated with MS Office/ OneDrive and therefore first choice as second strategic filesharing platform.
- With ownCloud you avoid a risky and expensive vendor-lock-in.
- ownCloud is open and flexible such that there's no need for expensive individual solutions for special use cases.
- ownCloud is the largest open source filesharing solution in the world with 50+ Million users. It's backed by the ownCloud foundation which guarantees the sustainability of the solution.

Annex

Data that can not be stored in MS OneDrive due to the Cloud Act:

All data that is subject to the obligation oft the GDPR (article 35) to do a Data Protection Impact Assessment (DPIA) can not be stored in MS OneDrive as the US government might have access to it under the Cloud Act.

The national Data Protection Authorities (DPA's) define the kind of data that fall under article 35.

The GDPR grants DPAs certain flexibility to determine when companies under their jurisdiction must – or need not – conduct a DPIA. Article 35(4) permits DPAs to issue "blacklists", i.e. lists of processing activities that always require a DPIA.

A full list of European DPA's blacklists can be found here: https://iapp.org/resources/article/eu-member-state-dpia-whitelists-and-blacklists/

About ownCloud

ownCloud is the market leading open source content collaboration solution worldwide. ownCloud enables users to securely access and share data from any device, anywhere in the world. With more than 200,000 installations and 50 million users, ownCloud provides organizations a modern collaborative experience, thereby boosting productivity without compromising on security. At the same time, it gives organizations the visibility and control required to manage sensitive data.

To get the latest updates, please visit https://owncloud.com/newsroom or follow us on Twitter @ownCloud.

ownCloud GmbH
Rathsbergstr. 17
90411 Nürnberg
Germany

Contact:
owncloud.com/contact
Phone: +49 911 14888690
owncloud.com

@ownCloud
facebook.com/owncloud
linkedin.com/company/owncloud