ownCloud Architecture Overview

Providing Access to Data Where It Lives

Your IT landscape is complex, and often inherited. You have storage systems, servers, private cloud management tools, log managers, backup tools, authentication options and many more solutions already deployed. You don't want to add another silo to enable secure file sharing for your employees, but you also don't want your corporate confidential information being passed around in consumer-grade applications across multiple devices. You are looking for an answer that lets you leverage your existing infrastructure without duplicating or moving data. Further, you are looking to regain control while enabling modern on-the-go access that is demanded by your workforce.

ownCloud provides Universal File Access through a common file access layer regardless of where the data lives – in applications, object stores, on-premise storage or in the cloud. Data is kept where it is while IT is able to manage proprietary information and business risk; leveraging existing data management, security and governance tools and processes. Whether in SharePoint, on a Windows network drive or in cloud storage, users have a single interface from which they can access, sync and share files on any device, anytime, from anywhere – all completely managed, secured and controlled by IT as seen in Figure 1.

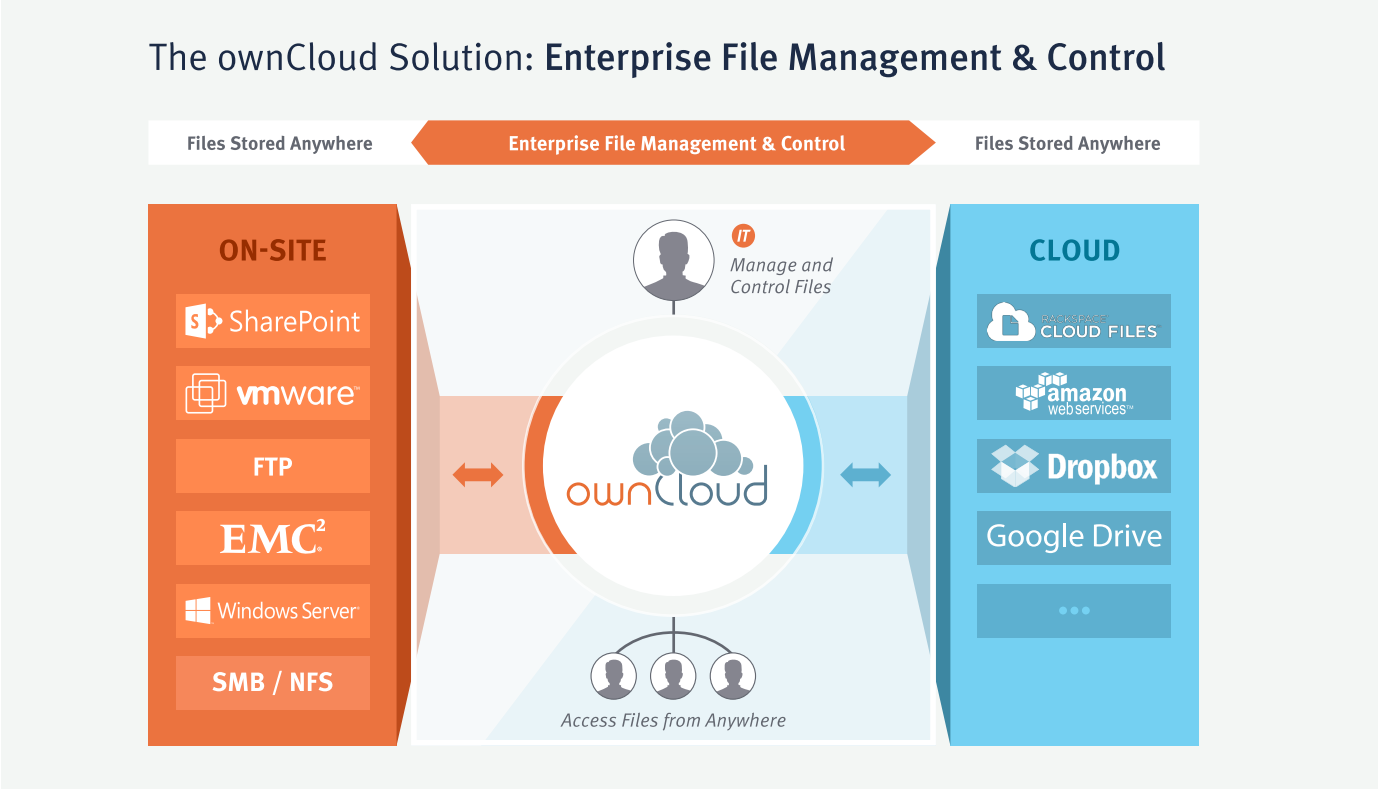

Figure 1: ownCloud has a single interface from which users can access, sync and share files on any device, anytime, from anywhere.

Solution Architecture Overview

The core of the ownCloud solution is the ownCloud server. Unlike consumer-grade file sharing services, ownCloud's server enables IT to protect and manage files within the ownCloud environment – from file storage to user provisioning, file access rules to file processing. ownCloud monitors and logs all data access events for downstream auditing and analysis using popular SIEM tools like Splunk®. The server provides a secure web interface through which administrators control all of ownCloud's resources, allowing authorized users to enable and disable features, set policies, federate servers, create backups and manage users. Advanced features for enterprise directory integration and file "firewall" rules give admins exceptional flexibility and control. The server also manages and secures API access to ownCloud, while providing the scalable processing engine needed to deliver high performance file sharing services.

The ownCloud server stores user files in

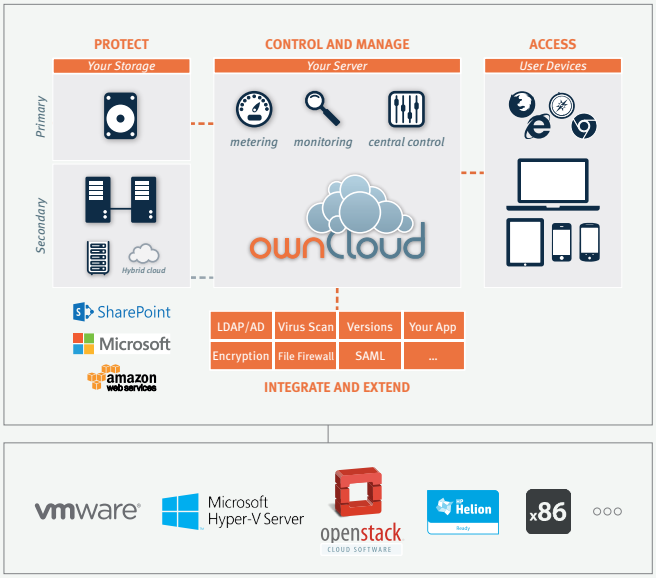

Figure 2: ownCloud Solution Architecture

standard file system formats and can use most enterprise file systems. If you can mount the file system on your server, ownCloud can use it. Further, ownCloud can also use S3 and Swift based object stores or compliant gateways – **ownCloud is filesystem and storage agnostic**. ownCloud can leverage storage that is physically located in your data center or "virtually mounted" third-party storage (Figure 2). Thus, ownCloud enables you to protect your files as you would any other data asset in your infrastructure. As demonstrated in Figure 3, ownCloud works seamlessly with your existing tools and utilities, from standard backups and intrusion detection, to log managers and Data Loss Prevention (DLP) solutions. ownCloud
can also activate the included encryption module to provide an added layer of encryption at rest for user files. ownCloud applications make integration with your existing technology stack a breeze. Enabled through the server control panel, integration plugins provide functionality such as Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) integration for user account provisioning, authentication and even quota management. SAML IdPs can also be used for authentication within ownCloud. For custom integrations, ownCloud can be easily extended using mobile libraries, external REST APIs, internal app development APIs and plugin applications. Features such as the online text editor, virus scanning, file versioning and server-side encryption are included in the ownCloud core. Features such as enhanced logging and audit plug-ins, File Firewall, Retention, SAML authentication and Windows network drive(s) integration, SharePoint integration and autotagging are available in the ownCloud Enterprise Edition.

ownCloud customers have integrated a wide variety of new functionality into ownCloud, from video streaming to contact and calendar syncing, custom authentication mechanisms, and API-based storage. Also, ownCloud's encryption model is highly scalable and allows administrators to maintain complete control over their encryption keys. In short, unlike proprietary alternatives, ownCloud can be easily extended to do far more than basic file sync and share.

While ownCloud provides the ability to access, control and protect data in the enterprise, ownCloud also delivers the consumer grade experience users expect on desktops, laptops, tablets and mobile phones. Intuitive interfaces guide end-users through a wide range of file sharing activities, and administrator efficiency is aided through wizards, management tools and monitoring and logging capabilities. ownCloud also provides the ability for standard WebDAV clients to access ownCloud files, enabling users to continue to use standards-based productivity tools to interoperate seamlessly with ownCloud.

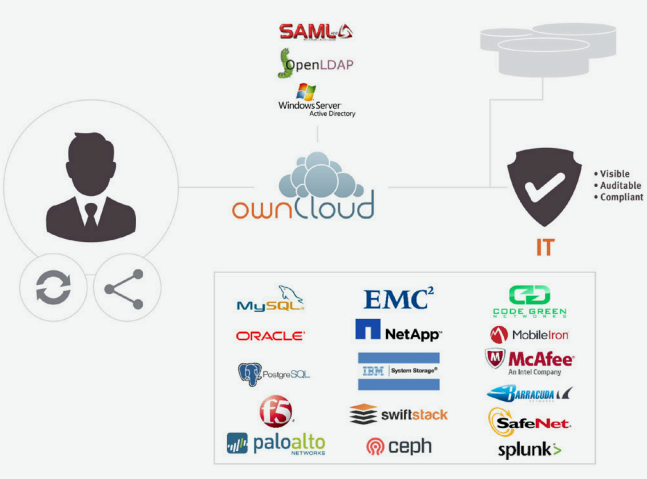

Figure 3: IT Controls Access in Their Environment

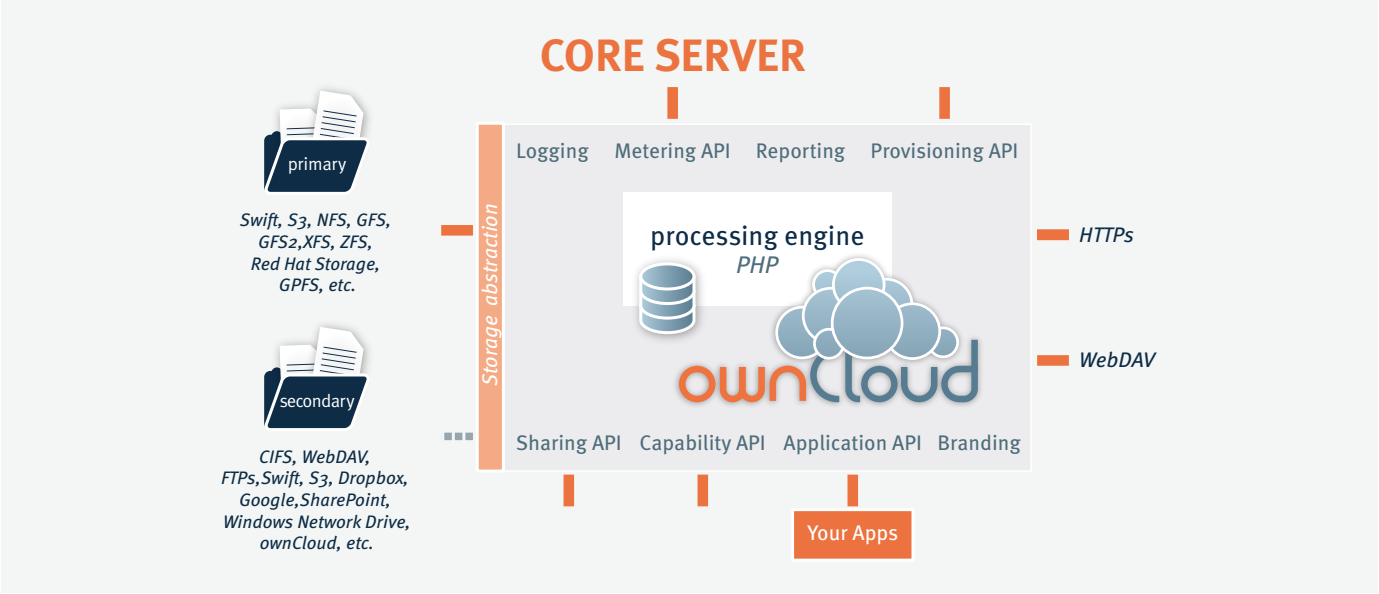

Figure 4: ownCloud Server Architecture

Server Architecture Overview

At its core, ownCloud is a PHP web application running on top of Apache on Linux. This PHP application manages every aspect of ownCloud, from user management to plugins, file sharing and storage. Attached to the PHP application is a database where ownCloud stores user information, user-shared file details, plugin application states, and the ownCloud file cache (a performance accelerator).
ownCloud accesses the database through an abstraction layer, enabling support for Oracle, MySQL and PostgreSQL. Complete webserver, user and system logging is provided and may be used with the log reporting tools of your choice.

To enable a broad range of storage alternatives, ownCloud also abstracts the storage tier. As a result, ownCloud can leverage just about any storage protocol that can be mounted on your ownCloud server – from CIFS, NFS and GFS2, to clustered file systems like Red Hat Storage, IBM Elastic Storage, and even object stores like Swift and S3. Other storage resources can also be mounted on the system using optional plug in applications, such as SharePoint, Windows network drives, Windows home directories, (s)FTP, WebDAV, another ownCloud instance and even external cloud storage services such as S3, Swift, Google Drive and Dropbox if desired. User configurations can include dynamically allocated storage driven by user directory entries – enabling data segregation and multitenant style deployments.

ownCloud includes a variety of open server-side APIs for integrating with other systems. These include:

- **Activity** – an RSS feed delivers all activities associated with a user's files, such as sharing activity, updated, renamed, deleted and removed files.

- **Applications** – the most powerful API, enabling customers to expand ownCloud out of the box, to integrate with existing infrastructure and systems, and to create new plugin applications. Examples of this API in use include the custom authentication backends, music and video streaming applications, a URL shortener app and an image preview application.

- **Capability** – information about the installed ownCloud capabilities, allows ownCloud and third-party applications to query for the enabled features and plugin applications.

- **External provisioning** – the ability to add and remove users remotely, and to query metering information about ownCloud storage usage and quota.

- **Sharing** – the ability for external apps, such as the ownCloud mobile app, to share files from remote devices or to natively share between two ownCloud servers.

- **Branding** – a simplified mechanism for branding ownCloud servers, and through *ownBrander*, to brand desktop, mobile and web clients to match your corporate look and feel.

In addition to delivering the core of ownCloud, the ownCloud server also includes the ownCloud web interface, which provides a control center for configuring, managing and monitoring the system.
ownCloud gives end users tools for controlling access to their files and folders. Employees are set up in the system as users, administrators, or both. Administrators can add, enable, and disable ownCloud features through the settings menu such as add and remove users and groups or manage various ownCloud settings and administrative tasks (migration and backup, for example). Users access the web interface to browse and manage their files, and to set granular permissions on files and folders shared with others on the system. Users can also access enabled applications through the web portal, such as the activity stream, text editor and image preview, file and folder sharing, SharePoint document libraries,
Windows network drives, rollback of previous versions and much more. The ownCloud web interface is compatible with all major browsers on Windows, Mac OS and Linux machines.

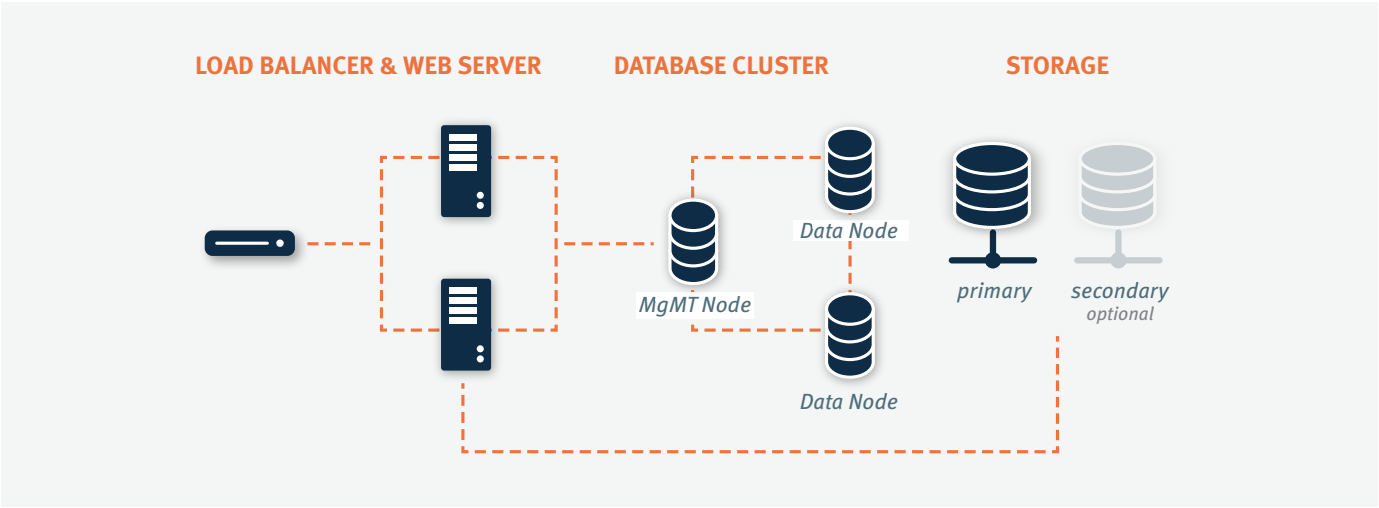

Figure 4: Common ownCloud Deployment Architecture

Deployment Scenario

With the ownCloud solution and server architectures outlined in Figure 2, this paper now examines how ownCloud is deployed on site, how it is integrated with the storage tier and existing infrastructure tools, and the flexibility provided by ownCloud's APIs. This understanding is facilitated by a brief review of how ownCloud is typically deployed in production environments.

In production, ownCloud is most often deployed as an n-tier load balanced web application running in a data center or managed cloud infrastructure. ownCloud can be deployed to physical, virtual, or private cloud servers using native binaries or a virtual appliance footprint. There is almost always a load balancer on the front-end of the deployment connected to at least two web servers for fault tolerance.

The ownCloud web servers host the PHP code, and are most often deployed on Apache over Linux. All of the web servers are then connected to a database (frequently a clustered Oracle or MySQL database instance) for user information, including the virtualized file cache, user and group meta data, shared file lists, and storage required by enabled ownCloud apps. The web servers are also all connected to shared backend storage, often a clustered filesystem. With this configuration, ownCloud can be scaled up easily to meet load requirements, while providing whatever redundancy and backup requirements are needed to achieve system availability objectives.

Onsite Storage

For nearly all deployment scenarios, connecting ownCloud to backend storage is as simple as mounting onsite storage on the server, such as mount point /data/storage_ device. Nearly all storage devices and file systems – from direct attached NTFS to cluster systems like Red Hat Storage – have well tested, high-performance Linux drivers that make this easy. Object stores can also be mounted through ownCloud. Once the storage device is mounted in the desired location, the ownCloud configuration file is edited with the storage device path, and all ownCloud storage is immediately changed to that path. Each user gets a directory, and all versions, folders and files are stored in that location. Object stores leverage containers in a similar manner, flattening the file path into the database and storing only an object.

In larger installations, it may be necessary to create more than one storage location for an ownCloud instance. Perhaps policy requires high performance, fully redundant storage for one group, and less expensive storage for another group. In this situation, it is possible to leverage ownCloud‘s built in integration with LDAP or Active Directory servers to dynamically assign a storage path to each user. The LDAP/AD plugin is further described below, but once connected, the storage path attribute can be inherited, and users can be directed to two or more storage paths based on these entries. Simply mount the storage devices on the server in the desired mount point, such as /data/high-endstorage1 and /data/lowendstorage2, and user files and versions will be saved to the specified path.

Occasionally ownCloud needs to connect to REST API-based storage. In some cases, API-accessed storage replaces the mounted file system described above, and in some cases it augments the storage. ownCloud can handle either scenario through the use of plugin applications. For example, ownCloud provides a plugin application that mounts S3 and Swift as HTTP based backend storage systems. When enabled, the plugin application performs all file operations using the abstracted S3 intervace. For the other folders on the server, ownCloud retains a file system mount. In other installations, ownCloud‘s built-in External Fileystem plugin leverages a mix of APIs, providing system admins the flexibility to connect CIFS, FTPs, WebDAV and other storage systems in addition to the existing filesystem storage.

Ultimately, administrators must decide which storage system(s) to use, how to configure user access, and whether or not to mix and match storage to optimize existing infrastructure, security policies, and end-user requirements. ownCloud provides the mechanisms to optimize the use of onsite, cloud or hybrid storage, giving admins control of corporate data, while still providing the capabilities that users demand.

For more information on scaling ownCloud and hardware sizing, visit owncloud.com/whitepapers

Infrastructure Integration

The most common infrastructure integration request is to connect ownCloud to an enterprise directory, or other standard authentication mechanisms. ownCloud provides out-of-the-box integration with LDAP, AD and SAML 2.0. Administrators simply enable the ownCloud LDAP/AD or SAML plugin application, configure the server addresses, protocols and filters, and users are authenticated against the appropriate service. With the appropriate settings, user group memberships, quotas and even, as seen in Figure 4, storage paths can be centrally managed and applied to ownCloud. It is even possible to enable SAML and AD/LDAP at the same time, using SAML for authentication and AD/LDAP for group memberships.

The first time a user logs into ownCloud with a user name and password, ownCloud provisions the user and they are off and running. Administrators can also enable custom attributes, such as custom display names and avatars to make it easier for users to find each other when sharing documents. All corporate policies governing the account, such as failed login account lockout, are still managed out of the corporate directory, with ownCloud enforcing the result.

Beyond LDAP/AD integration, ownCloud offers a wide range of other integration capabilities. For example, it is possible to leverage the user provisioning API to provision new users via an external automation service. In some very large deployment scenarios, it is far more efficient to provision new users in this manner than to use an enterprise directory. The provisioning API can also be used to report on user activity, shared file information, and to disable user accounts. The WebDAV API can be used to provide authenticated access to ownCloud files and folders based on user accounts, a popular feature among tablet users. WebDAV support also allows desktop users to browse ownCloud folders using familiar file explorer tools in Windows, Mac and Linux. While most deployed customers limit themselves to LDAP/AD integration and WebDAV access, ownCloud APIs offer the flexibility to integrate as needed into existing environments.

ownCloud also provides mechanisms for creating plugin applications to integrate with existing systems. One common use case is the custom authentication mechanism. While ownCloud supports LDAP and AD integration and SAML 2.0, several custom user authentication and authorization plugins have been created, from token to user name and password-based plugins. Others integrations have included log managers, Data Loss Prevention (DLP) tools, Mobile Device Management (MDM) tools and antivirus mechanisms, to name a few.

ownCloud also offers integrations with SharePoint, Windows network drives as well as other ownCloud instances. Access Control Lists (ACLs) and local policies are preserved and files are synced automatically in both directions. Selective sync allows users to sync only the most relevant files which are all accessible through the ownCloud interface and, subsequently, on any device. Users may also configure web and desktop clients for a single view into multiple ownCloud instances.

As an n-Tier web application, ownCloud integrates into most corporate web farms. Intrusion detection systems, network management tools and firewalls simply leverage existing ports and SSL certificates. Backup systems take server and database backups as with any other web application, and user experience systems wrap around the existing ownCloud application. For unique requirements, the ownCloud API's and mobile libraries provide extensive flexibility. All of this gets managed with enterprise tools, in an enterprise data center, to enterprise policies, putting IT back in control of corporate data, while providing end users the pleasing, productive interfaces they demand.

Data protection is also a critical requirement for sharing files. ownCloud provides robust server-side encryption for data at rest. ownCloud's open architecture also integrates with toolkits such as OpenSSL to protect in-flight data, and can be easily extended to support other advanced security requirements such as client-side encryption.

Additional flexibility is also inherent in the encryption that is available in ownCloud. Customers are provided the ability to manage their key stores and to access/manage the reading and writing of files. Admins choose and implement the key manager of their choice (theirs, ours or a different one altogether) or replace the AES-256 cipher with one of their choosing. ownCloud is the only vendor to provide this capability. ownCloud Encryption 2.0 is built modularly with the ability to swap out components. Encryption is delivered as an app that is easily and quickly integrated with existing infrastructure.

Conclusion

ownCloud is open by nature and designed to integrate with existing infrastructure, management and security tools. A comprehensive set of APIs and native integrations enable anytime, anywhere access to all your data, wherever it resides.

For More Information

Please visit www.owncloud.com for more information about ownCloud product downloads, and detailed product documentation.

ownCloud GmbH
Leipziger Platz 21
90491 Nürnberg
Germany

www.owncloud.com/contact
phone: +49 911 14888690

www.owncloud.com

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