ownCloud Architecture Overview

ownCloud, Inc.
57 Bedford Street, Suite 102
Lexington, MA 02420
United States

phone: +1 (877) 394-2030
www.owncloud.com/contact

ownCloud GmbH
Schloßäckerstraße 26a
90443 Nürnberg
Germany

Tel.: +49 911 21 64 50 79
www.owncloud.com/de/contact

ownCloud Architecture Overview

Sensitive enterprise data is outside of IT‘s control

Many employees use cloud-based services to share sensitive company data with each other, vendors, customers and partners. They sync data to their personal devices and home computers in an effort to do their jobs quickly and efficiently – without IT‘s oversight. Consumer cloud-based file sharing services store sensitive company data on external servers outside of IT’s control, in violation of corporate policies and regulatory requirements – maybe even outside the country – and not managed by IT. The risks of data leakage, compliance violations and damage to the business are enormous.

The Dropbox Problem in Action

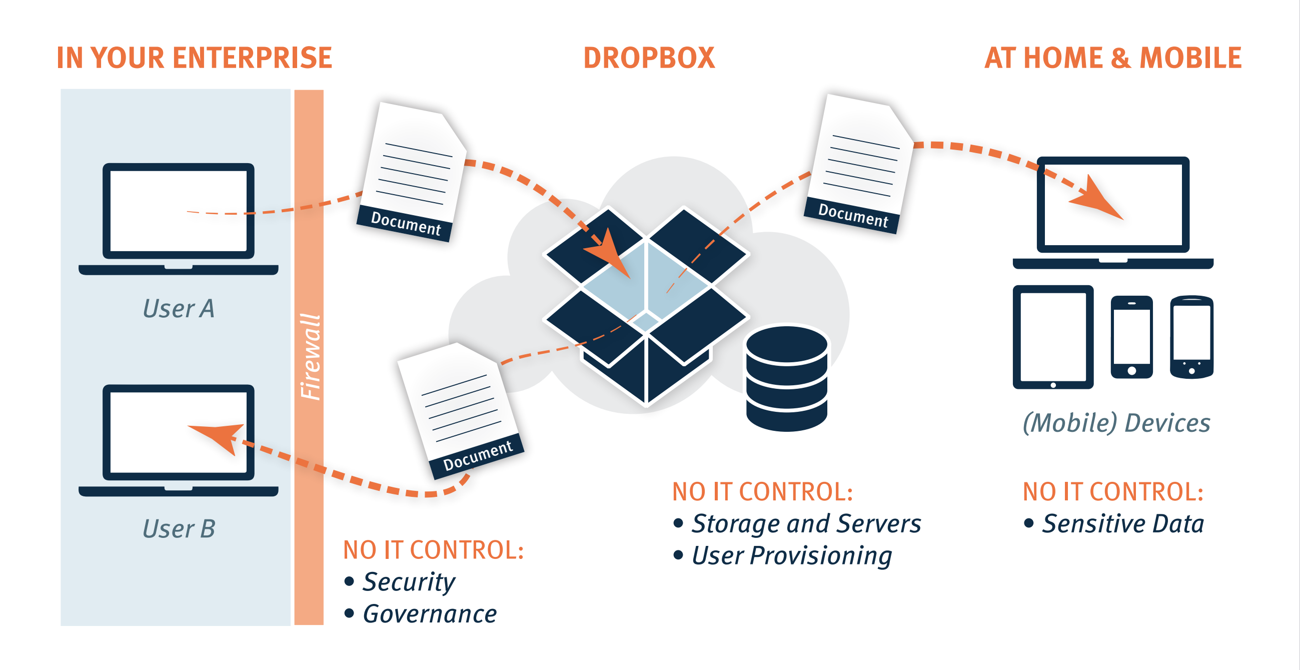

Figure 1: How sensitive data is shared beyond the firewall and IT control

Time to Regain Control

ownCloud allows IT to regain control of sensitive data with managed file sync and share:

- **Manage and Protect** data on-premise – using any available storage, with the complete software stack running on servers safely inside the data center, controlled by trusted administrators, managed to established policies.
- **Integrate** with existing IT systems and policies – such as authentication systems, user directories, governance workflows, intrusion detection, monitoring, logging and storage management.
- **Extend** functionality easily through a comprehensive set of APIs to customize system capabilities, meet unique service requirements, and accommodate changing user needs.

AND STILL provide end users clean, intuitive access to the documents they need to get the job done using desktop systems, laptops, tablets and smart phones.

ownCloud in Action

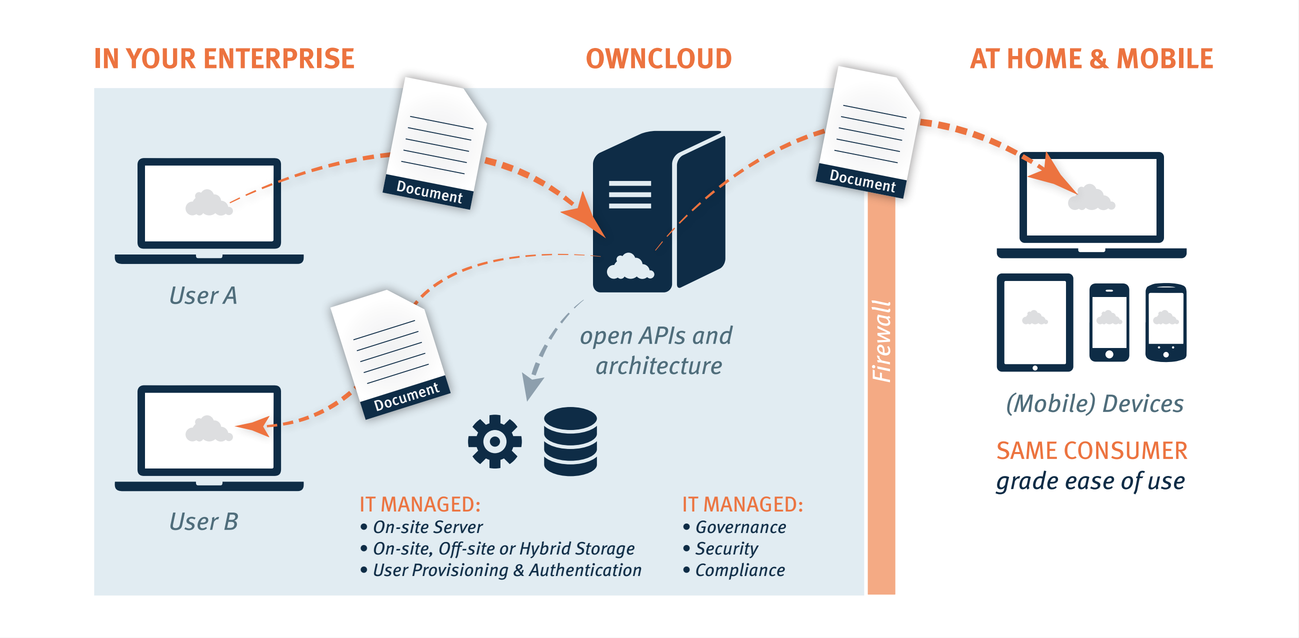

Figure 2: ownCloud provides managed file sync and share AND STILL consumer-grade usability

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 and data processing. ownCloud monitors and logs all data access events for downstream auditing and analysis using popular 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, create backups and manage users. Advanced features for enterprise directory integration and file “firewalls” give admins exceptional flexibility and control. The server also manages and secures API access to ownCloud, while providing the internal processing engine needed to deliver high performance file sharing services.

The ownCloud server stores user files in 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 – ownCloud is file system and storage agnostic. ownCloud can leverage storage that is physically located in your data center or “virtually mounted” third-party storage. Thus, ownCloud enables you to protect your files as you would any other data asset in your infrastructure. ownCloud works seamlessly with all of 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 provided plug-in applications make integration with your existing technology stack a breeze. Enabled through the server control panel, integration plug-ins provide functionality such as Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) integration for user account provisioning and authentication. For custom integrations, ownCloud can be easily extended using mobile libraries, open APIs and plug-in applications. Features such as the online text editor, virus scanner, file versioning and server-side encryption are included in the ownCloud core. Enterprise features such as enhanced logging and audit plug-ins, File Firewall, SAML authentication and Jive Software® integration 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, automated Optical Character Recognition back ends, and API-based storage. In short, unlike proprietary alternatives, ownCloud can be easily extended to do far more than basic file sync and share.

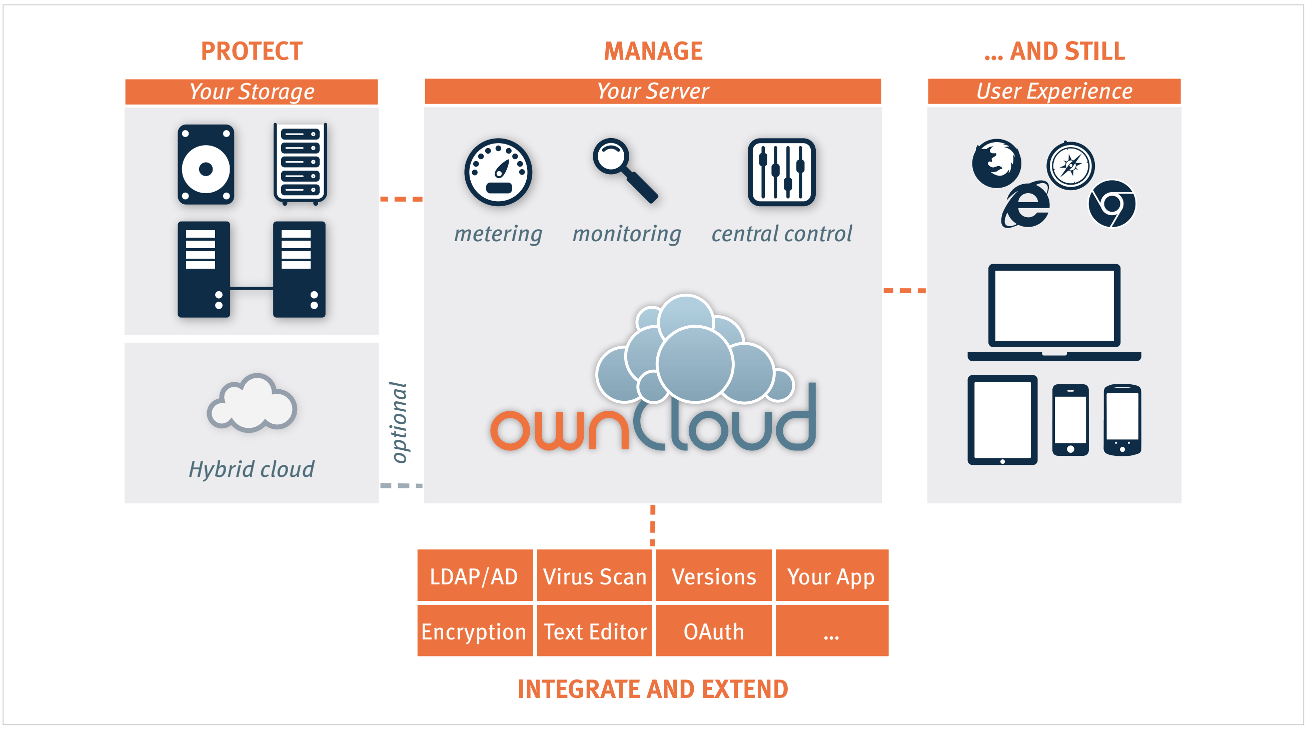

Figure 3: ownCloud Solution Architecture

While ownCloud provides the ability to **Manage and Protect**, **Integrate** and **Extend** file sync and share in the enterprise, ownCloud also delivers the **crisp, professional user experience** on desktops, laptops, tablets and mobile phones that users demand. Intuitive, eye-pleasing visualizations guide end users through a wide range of file sharing activities, and high-productivity wizards, management and monitoring screens allow ownCloud administrators to operate with efficiency. 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.

Server Architecture Overview

At its core, ownCloud is a PHP web application running on top of IIS or Apache on Windows or Linux. This PHP application manages every other aspect of ownCloud, from user management to plug-ins, file sharing and storage. Attached to the PHP application is a database where ownCloud stores users, user-shared file details, plug-in application states, and the ownCloud file cache (a performance accelerator). ownCloud accesses the database through an abstraction layer, enabling support for Oracle, MySQL, SQL Server, and PostgreSQL. Complete webserver logging is provided via webserver logs, and user and system logs are provided in a separate ownCloud log, or can be directed to a syslog file.

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. Other storage resources can also be mounted on the system using optional external file system applications, such as Jive, Windows Home Directories, FTPs, WebDAV and even external cloud storage services S3, Swift, Google Drive and Dropbox if desired. User configurations can include dynamically allocated storage driven by user directory entries – enabling data segregation and multi-tenant deployments.

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

- **Activity** – provides an RSS feed or API call to deliver 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 plug-in applications. Examples of this API in use include the custom

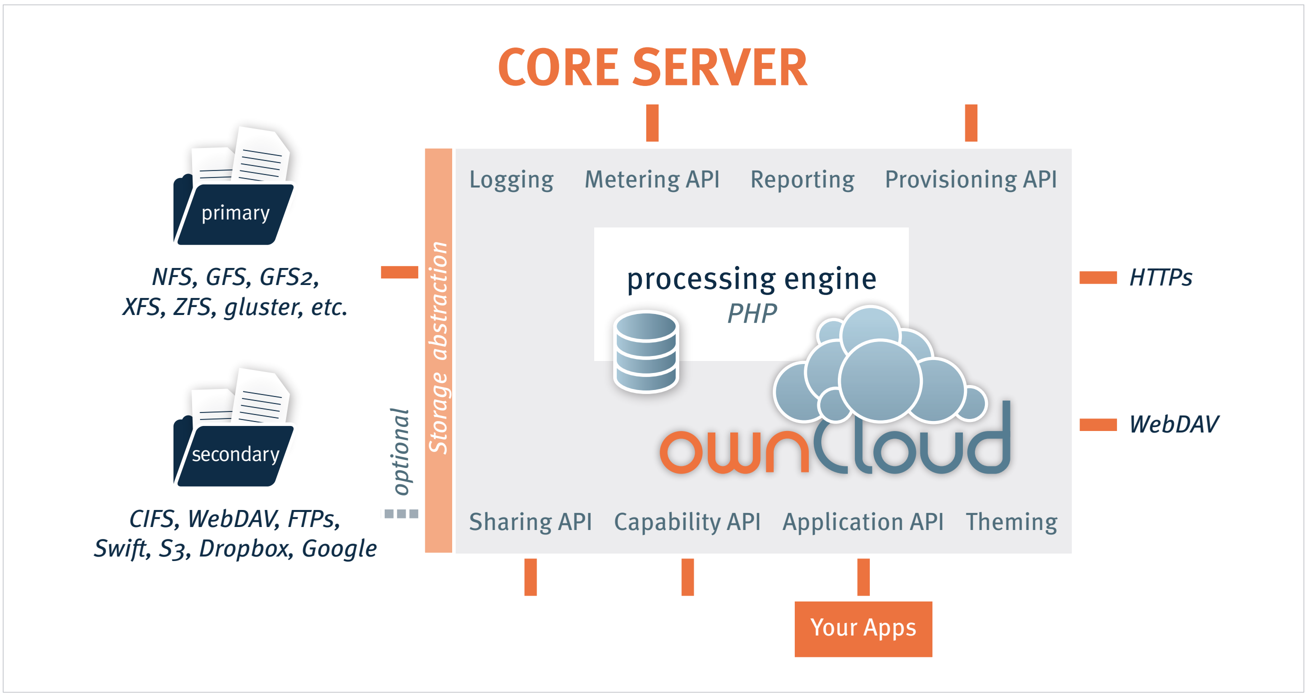

Figure 4: ownCloud Server Architecture

authentication back ends, music and video streaming applications, a bit.ly-inspired app called shorty, and an image preview application.

- **Capability** – offers information about the installed ownCloud capabilities, so that ownCloud and third party applications can query for the enabled features and plug-in applications.
- **External provisioning** – provides the ability to add and remove users remotely, and enables admins to query metering information about ownCloud storage usage and quota.
- **Sharing** – provides the ability for external apps, such as the ownCloud mobile app, to share files from remote devices.
- **Themeing** – a simplified mechanism for branding the ownCloud server to match your corporate look and feel, enabling colors and logos to be updated with style sheets.

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. The ownCloud portal also 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; they can add and remove users and groups; and they can 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 text and image previews, file and folder sharing, Jive integration, previous versions roll back, and much more. The ownCloud web interface is compatible with Firefox, Safari, Chrome and Internet Explorer on Windows, Mac OS and Linux machines.

Deployment Scenario

With the ownCloud solution and server architectures outlined above, 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 always a load balancer on the front-end of the deployment connected to at least two web servers. The ownCloud web servers host the PHP code, and are most often deployed on Apache over Linux, though IIS and Apache on Windows are also supported. All of the web servers are then connected to a

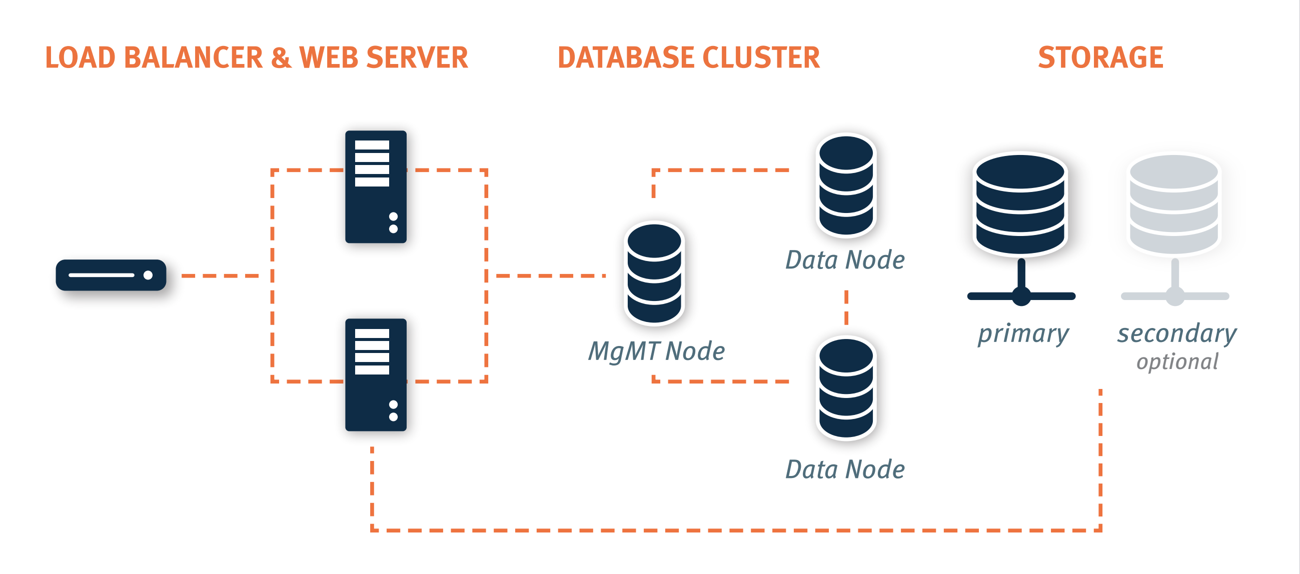

Figure 4: Common ownCloud Deployment Architecture

database (frequently a clustered 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 back-end 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.

On-Site Storage

For nearly all deployment scenarios, connecting ownCloud to back-end storage is as simple as mounting on-site 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. 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.

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 plug-in 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 plug-in applications. For example, ownCloud provides a plug-in application that mounts Jive as a backend storage location via Jive Rest APIs. When enabled, the plug-in application redirects POSIX commands for one folder of user content to the Jive REST API. For the other folders on the server, ownCloud retains a file system mount. In other installations, ownCloud‘s built-in External Fileystem plug-in leverages a mix of APIs, providing system admins the flexibility to connect openStack SWIFT, CIFS, FTPs, WebDAV and other storage systems in addition to the existing file system storage.

Ultimately, administrators must decide which storage system 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 on-site, cloud or hybrid storage, giving admins control of corporate data, while still providing the capabilities that users demand.

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 AD / LDAP or SAML plug-in 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 outlined above, storage paths can be centrally managed and applied to ownCloud. 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, 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 account information, 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 plug-in 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 plug-ins have been created, from token to user name and password-based plug-ins. Others integrations have included log managers, Data Loss Prevention tools, and antivirus mechanisms, to name a few.

As an n-Tier web application, ownCloud integrates into most corporate web farms. Intrusion detection systems work, network management tools work, 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, to put IT back in control of corporate data, and still provide end users the pleasing, productive interfaces they demand.

Conclusion

Many employees use cloud-based services to share sensitive company data with each other, vendors, customers and partners. They sync data to their personal devices and home computers, all in an effort to do their jobs quickly and efficiently – all without IT's oversight. With ownCloud, you can **Manage and Protect** sensitive data by hosting your own solution on site, using your own storage and servers; **Integrate** seamlessly into existing infrastructure, management and security tools; **Extend** functionality easily through a comprehensive set of APIs, **AND STILL** provide the polished, professional user experiences employees have come to value from consumer-grade services, running on all popular desktop and mobile devices.

But don't take our word for it, point your browser to www.ownCloud.com and take ownCloud for a test drive today.

For More Information

Please visit our website at **www.owncloud.com** for a wealth of information about ownCloud, links to download the software, and detailed product documentation.

US Headquarters
ownCloud, Inc.
57 Bedford Street, Suite 102
Lexington, MA 02420
United States

www.owncloud.com/contact

European Headquarters
ownCloud GmbH
Schloßäckerstraße 26a
90443 Nürnberg
Germany

www.owncloud.com/de/contact

ownCloud, Inc.
57 Bedford Street
Suite 102
Lexington, MA 02422
United States

www.owncloud.com/contact
phone: +1 (877) 394-2030

ownCloud GmbH
Schloßäckerstraße 26a
90443 Nürnberg
Germany

www.owncloud.com/de/contact
Tel.: +49 911 21 64 50 79

www.owncloud.com