



OpenCloud

Highest security for your data

Security

<https://opencloud.eu>



Table of contents

03	OpenCloud - Highest data security
04	Where conventional systems reach their limits
05	Principles of a secure file management platform
06	Architecture and security model of OpenCloud
09	Identity and authorisation management
11	Multi-layered protection against malware in OpenCloud
12	Essential security features of OpenCloud
13	Advantages over PHP-based solutions
14	Compliance and digital sovereignty with OpenCloud
15	Your choice for digital sovereignty

OpenCloud - Highest data security

Security in file management is no longer a nice-to-have—it's a must. Cyberattacks, data leaks, and ever-tighter compliance rules are turning up the heat on organizations everywhere. In the public sector, in critical infrastructure, and in research institutions, even a single weak spot can cause reputational damage, legal trouble, or disrupt essential operations.

OpenCloud addresses precisely those security and compliance requirements that conventional systems fail to meet. The platform offers a secure, auditable environment for file management and digital collaboration – without the typical vulnerabilities of classic PHP-based systems. Instead of dynamically interpreted scripts, OpenCloud relies on compiled code in signed containers, a strictly separated three-tier architecture and multi-layered security mechanisms.

OpenCloud combines open standards with a comprehensive security concept. Multi-tenancy, differentiated access control and comprehensive audit functions ensure secure and traceable operation – even in highly sensitive or federal environments.

OpenCloud is based on a fork of the open source software 'ownCloud Infinite Scale' (OCIS), whose components were co-developed by developers from the science organisation CERN and other active contributors. OpenCloud is now being further developed by the Heinlein Group with new ideas and a clear focus on data protection, interoperability and sustainable digitalisation.

Where conventional systems reach their limits

In the public sector, in critical infrastructure and in research, strict security and compliance rules apply everywhere. Yet many platforms still show the same weaknesses:

- Insecure file uploads with little or no control over file size
- Unclear or poorly defined access rights
- Large attack surfaces caused by complex dependencies and missing isolation

Many PHP-based systems interpret source code at runtime. This opens the door for attackers to inject malicious code and execute it directly during operation. The lack of signatures makes it even harder to verify integrity. And without air-gapped operation, fully isolated network environments are simply not an option.



Principles of a secure file management platform

Maximum security is not achieved through individual functions, but through a security concept that extends from the foundation to the last interface.

For organisations with high security requirements, three principles are key:

- 1. Defense-in-Depth:**
Several layers of protection, from the overall architecture down to file verification, make attacks harder and limit their impact.
- 2. Least Privilege:**
Access is granted only when truly needed, with clear separation of roles and rights.
- 3. Auditability and digital sovereignty:**
Every access is fully traceable, stays entirely with the organisation in charge.

Platforms built on these principles not only offer effective protection against today's threats, but also remain adaptable to future security and compliance requirements.

OpenCloud consistently implements these security principles – from architecture and operation to individual protection mechanisms.

The following sections show in detail how the platform resists threats, meets compliance requirements and at the same time ensures full control over data and infrastructure.

Architecture and security model of OpenCloud

OpenCloud is designed with security, transparency and full data control at its core. The platform follows a modern three-tier architecture and combines proven cloud-native principles with carefully chosen design decisions to minimise the attack surface and keep operations simple.

Three tiers for maximum control

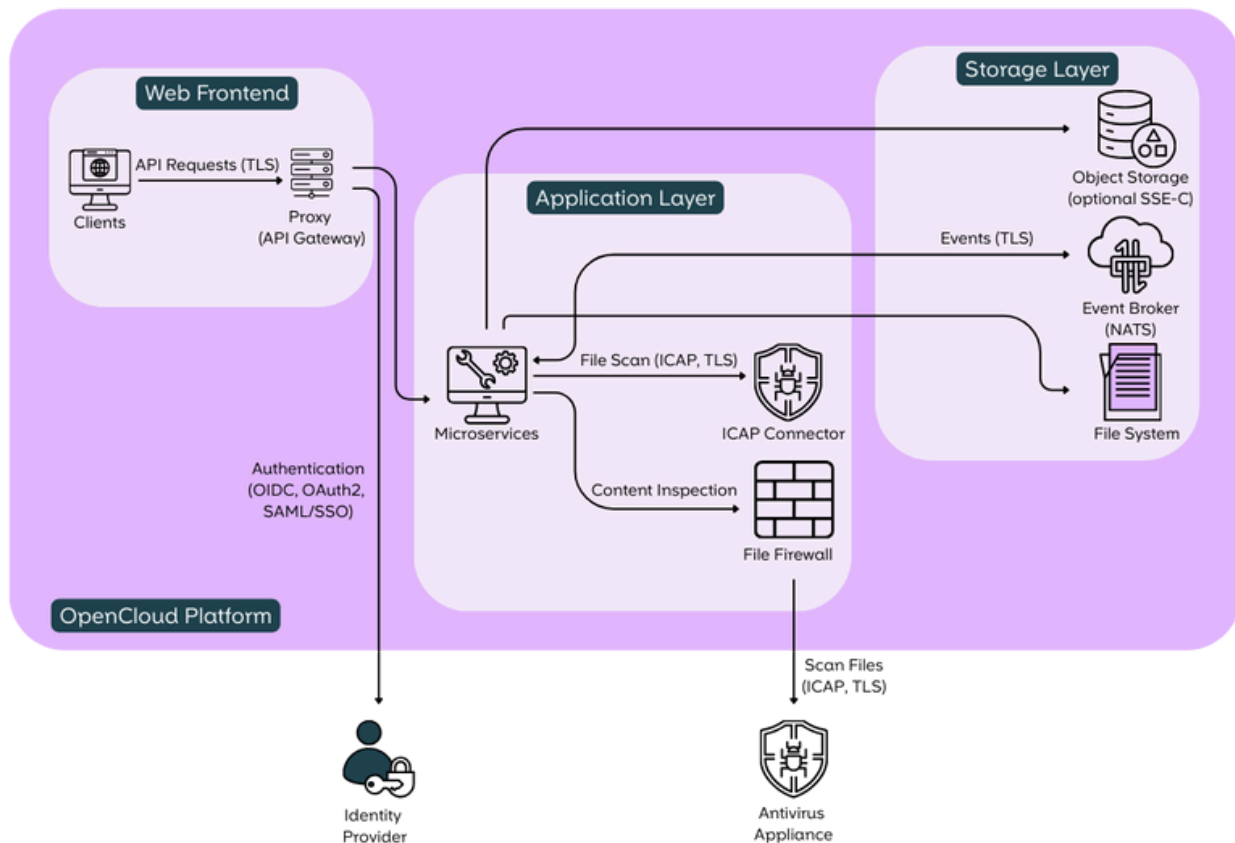
OpenCloud strictly separates the web front end, application layer and storage layer from each other. All requests first run through an upstream proxy, which acts as an API gateway and only allows authorised access. The application layer consists of modular microservices that communicate with other services via secure TLS connections.

The storage layer manages all files and metadata. This involves the use of a connected object storage system (optionally with SSE-C encryption), the file system and the NATS event broker. NATS handles the secure, TLS-encrypted exchange of messages between the application and the storage system.

This design ensures clear responsibilities and prevents attacks or errors from spreading laterally within the system. OpenCloud consistently encrypts all connections between services and layers with TLS – both internally and externally

Architecture and security model of OpenCloud

Secure Architecture of OpenCloud



Compiled code instead of dynamic execution

OpenCloud does not use dynamically interpreted languages such as PHP, relying instead on compiled code that is delivered exclusively in signed containers. Changes to the system require rebuilding and re-signing.

This prevents manipulation during runtime – a key difference to traditional web applications that interpret source code directly. The mandatory build and signature process significantly reduces the attack surface, as no external scripts or modules can be spontaneously introduced into the system.

Architecture and security model of OpenCloud

Data storage without a database

OpenCloud stores all metadata directly in the file system or in a connected object storage. This means that an (SQL) database is not required, eliminating attack vectors such as SQL injection.

At the same time, the platform is easier to secure: since OpenCloud does not use a database, a snapshot of the file system or object storage is sufficient to create a complete backup.

In case of particularly high requirements, OpenCloud can be extended to support client-side encryption and the use of custom keys via SSE-C (Server-Side Encryption with Customer Keys). This would allow organisations to keep their keys completely under their own control

Trusted containers through signatures

All containers are cryptographically signed. During deployment, OpenCloud verifies that each image is authentic and unmodified. This ensures that no tampered or untrusted containers ever enter the system.

OpenCloud therefore prioritises the integrity of the software used and enhances security throughout the entire supply chain – from source code to production environment.

Identity and authorisation management

Anyone handling sensitive data needs reliable authentication and authorisation. OpenCloud provides a flexible, well-integrated system that fits smoothly into existing IT environments – from login to fine-grained access control.

Strong authentication and access control

All OpenCloud APIs are protected. The platform uses modern authentication methods and supports open standards like OpenID Connect (OIDC), OAuth 2.0 and Security Assertion Markup Language (SAML).

This makes it easy to connect OpenCloud to existing identity services such as Keycloak, LDAP or Active Directory—for example, for single sign-on (SSO) or two-factor authentication.

If there are special requirements, customised solutions can also be integrated, such as company-specific systems, token mechanisms, proprietary user databases or hardware-based authentication.

Organisations retain full control over their central user management and can continue to use existing authorisation concepts.

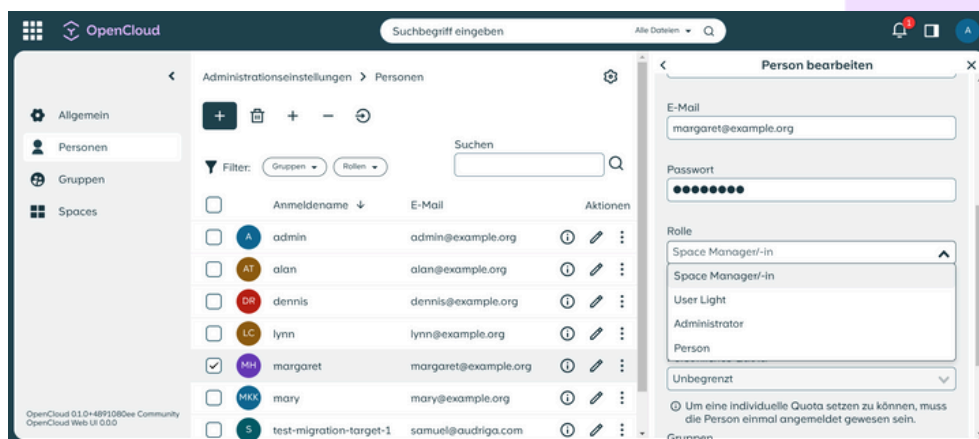


Fig.: OpenCloud granting rights to individual persons

Identity and authorisation management

Role-based rights management

OpenCloud follows the principle of role-based separation of duties: users who create a workspace (space) do not automatically have access to its contents. Reading, writing and administrative rights can be assigned independently.

This prevents sensitive data from being accidentally exposed or changed without permission. At the same time, administrators and managers always have a clear view of who can access what – an essential foundation for security and traceability in daily operations.

Flexible deployment options

OpenCloud adapts to its local environment – not the other way around. Whether in your own data centre, in a private cloud or completely isolated in air-gap operation, OpenCloud can be operated in accordance with the respective compliance requirements.

Control over location, network access and data storage remains entirely with the operating organisation. No external service provider and no third-country provider can access the environment. This makes OpenCloud particularly attractive for organisations with high protection requirements – such as in the public sector, in research or in security-critical infrastructures.

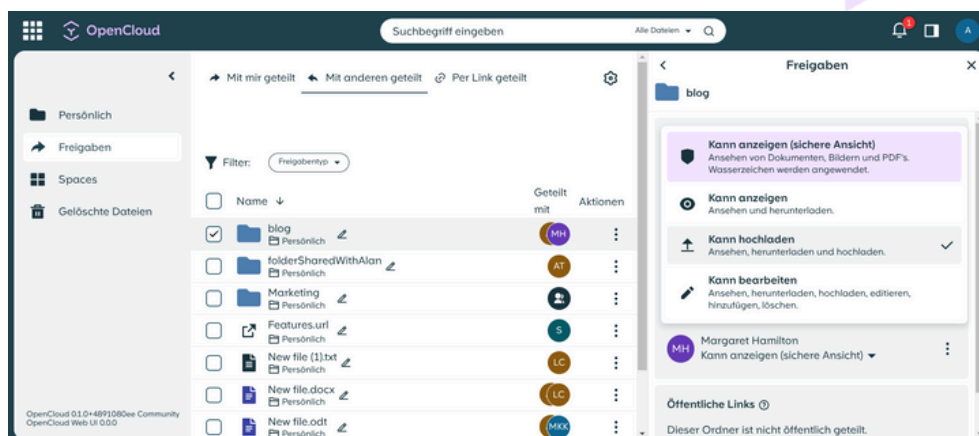


Fig.: OpenCloud view of shared files

Multi-layered protection against malware

File uploads are among the most common attack vectors in web-based systems. Malware, hidden scripts or disguised file types can cause serious damage – from data theft to full system compromise. OpenCloud addresses this risk with a multi-layered protection concept for all uploaded files.

Enterprise-grade malware protection

OpenCloud can be linked directly to company-wide virus protection solutions via the ICAP protocol (Internet Content Adaptation Protocol). Each upload is transferred in real time to an external virus scanner system, such as a dedicated appliance or a scan engine already present in the infrastructure. Only when the file has been classified as safe does OpenCloud accept it into the system – otherwise it remains in quarantine and is not distributed via shares.

This allows administrators to protect the cloud from malware, ransomware and other file-based attacks – while also meeting key IT security and compliance requirements.

Content-based file inspection

OpenCloud also checks the actual contents of files – regardless of their file extension. This means that a supposed image file with embedded malicious code will be detected, even if it is correctly named. This so-called file firewall delves deep into the data structure and detects discrepancies between the declared and actual file format.

Essential security features of OpenCloud

Function	Description
API authentication	All interfaces are secured with strong authentication (OIDC, OAuth2, SAML).
Separation of permissions	Permissions for creating and accessing workspaces (Spaces) are independent – no automatic full access.
Compiled code	Changes require compilation; prevents runtime manipulation and code injection.
Three-layer architecture	Web, application and storage are strictly separated.
Virus protection (ICAP integration)	Connection of external virus scanners via ICAP to check all uploads in real time.
Firewall for file contents	Content verification instead of just file extensions.
Signed containers	Only cryptographically verified images are executed; protects against supply chain attacks.
No database	All data is stored directly in the file system, reducing potential points of attack.
TLS encryption	All connections are fully TLS-encrypted – both internally and externally.
SSE-C & client-side encryption	Confidential data can be encrypted with your own keys and secured before upload.
Control over operation	Operation on-premises, in the private cloud or completely isolated (air gap).

Advantages over PHP-based solutions

Many conventional file management systems are based on PHP – a widely used but dynamically interpreted scripting language. OpenCloud deliberately takes a different approach here.

The platform is based on compiled code that is delivered as a signed container. This offers several security and stability advantages.

- 1. Less vulnerability, clearly regulated dependencies:**
No dynamic code execution, fewer vulnerabilities – dependencies are checked and secured during the development process.
- 2. No code injection through dynamic script execution:**
Compiled code cannot be manipulated at runtime. It is technically impossible to inject malicious code via forms, POST requests or eval() functions.
- 3. Greater stability and predictable performance:**
OpenCloud runs independently of host systems or PHP modules, but in signed, isolated container environments. This reduces side effects and ensures consistent performance – even during updates or under high load.

Compliance and digital sovereignty with OpenCloud

OpenCloud enables organisations to comply with regulatory requirements while retaining control over their data – regardless of cloud providers, jurisdictions or proprietary technologies.

OpenCloud meets the requirements of the GDPR and can be adapted to industry-specific regulations such as BSI basic protection or KRITIS requirements. Features such as logging, transparent rights assignment and flexible storage locations support data protection-compliant use.

All data remains completely under your control – regardless of whether you operate OpenCloud in your own data centre, in a private cloud or in a completely isolated environment (air gap). External service providers or third countries have no access.

Thanks to open standards, open-source components and a clear architecture, OpenCloud is auditable and maintainable in the long term. The platform is multi-tenant capable and can be easily integrated into federal or complex IT structures.

OpenCloud is therefore not only technically secure, but also creates the conditions for digital independence in the sense of a truly sovereign IT infrastructure.

Your choice for digital sovereignty

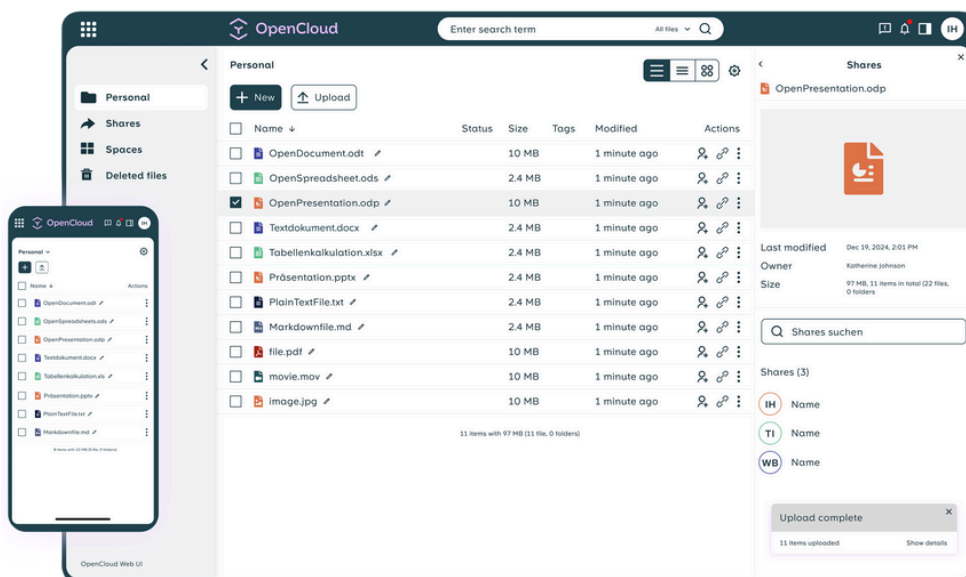
OpenCloud offers a secure, auditable platform for file management, file sharing and digital collaboration – developed for organisations with the highest requirements for data protection, control and flexibility.

The combination of compiled code, verified containers, flexible authorisation concepts and complete data sovereignty makes OpenCloud a future-proof platform. From its secure architecture to its support for air-gapped environments, OpenCloud meets all the requirements for sovereign, GDPR-compliant IT operations.

Rely on open source, open standards and full control – and choose a platform that fits your security strategy.

Protect your data with a platform that has been designed from the ground up for maximum security. Talk to us about your security strategy – we'll show you how OpenCloud can be seamlessly integrated into your infrastructure.

Get in contact with us at sales@opencloud.eu. We look forward to hearing from you.





OpenCloud

<https://opencloud.eu>

