OpenCloud

Höchste Sicherheit für Ihre Daten

Security

https://opencloud.eu

Inhalt

OpenCloud - Sicherheit für Ihre Daten

Sicherheit im File-Management ist heute keine Kür mehr – sie ist Pflicht. Cyberangriffe, Datenlecks und komplexe Compliance-Anforderungen setzen Organisationen zunehmend unter Druck. Ob im öffentlichen Sektor, in kritischen Infrastrukturen oder in sensiblen Forschungsbereichen – jede Schwachstelle kann gravierende Folgen haben: von Imageschäden über rechtliche Konsequenzen bis hin zum vollständigen Ausfall der Arbeitsfähigkeit.

OpenCloud adressiert genau die Sicherheits- und Compliance-Anforderungen, an denen herkömmliche Systeme scheitern. Die Plattform bietet eine sichere, auditierbare Umgebung für Datei-Management und digitale Zusammenarbeit – ohne die typischen Schwachstellen klassischer PHP-basierter Systeme. Anstelle dynamisch interpretierter Skripte setzt OpenCloud auf kompilierten Code in signierten Containern, eine strikt getrennte Three-Tier-Architektur und mehrschichtige Sicherheits-mechanismen.

OpenCloud vereint offene Standards mit einem durchgängigen Sicherheitskonzept. Mandantenfähigkeit, differenzierte Zugriffssteuerung und umfassende Auditfunktionen sorgen für einen sicheren und nach-vollziehbaren Betrieb – auch in hochsensiblen oder föderalen Umgebungen.

OpenCloud basiert auf einem Fork der Open Source-Software „ownCloud Infinite Scale“ (OCIS), dessen Komponenten u.a. von Entwickler*innen der Science-Organisation CERN sowie anderen Aktiven mitentwickelt wurden. OpenCloud wird nun von der Heinlein Gruppe mit neuen Ideen und einem klaren Fokus auf Datenschutz, Interoperabilität und nachhaltige Digitalisierung weiterentwickelt.

Wo herkömmliche Systeme an ihre Grenzen stoßen

Öffentlicher Sektor, kritische Infrastrukturen, Forschung – überall gelten strenge Sicherheits- und Compliance-Vorgaben. Typische Schwachstellen vieler Plattformen sind:

- Nicht validierte Datei-Uploads oft mit Größenbegrenzung der handhabbaren Dateien
- Unklare oder unzureichend differenzierte Zugriffsrechte
- Große Angriffsflächen durch komplexe Abhängigkeiten und fehlende Isolierung

PHP-basierte Systeme interpretieren Quellcode zur Laufzeit. Dadurch besteht das Risiko, dass Angreifer manipulierten oder unsicheren Code einschleusen und direkt im Betrieb ausführen lassen können. Fehlende Signaturen erschweren zusätzlich die Integritätsprüfung. Und ohne Air-Gap-Fähigkeit ist ein Einsatz in vollständig isolierten Netzwerken ausgeschlossen.

Prinzipien einer sicheren File-Management-Plattform

Maximale Sicherheit entsteht nicht durch einzelne Funktionen, sondern durch ein Sicherheitskonzept, das vom Fundament bis zur letzten Schnittstelle greift.

Für Organisationen mit hohen Schutzanforderungen sind drei Prinzipien entscheidend:

1. **Defense-in-Depth:**
   Mehrere Schutzschichten, von der Systemarchitektur bis zur Dateiprüfung, erschweren Angriffe und begrenzen die Wirkung.

2. **Least Privilege:**
   Zugriff nur, wenn er tatsächlich benötigt wird; klare Trennung von Rollen und Rechten.

3. **Auditierbarkeit und digitale Souveränität:**
   Jeder Zugriff ist lückenlos nachvollziehbar, die Datenhoheit bleibt vollständig bei der betreibenden Organisation.

Plattformen, die diese Grundsätze konsequent umsetzen, bieten nicht nur wirksamen Schutz vor heutigen Bedrohungen, sondern bleiben auch anpassungsfähig für künftige Sicherheits- und Compliance-Anforderungen.

OpenCloud setzt diese Sicherheitsprinzipien konsequent um – von der Architektur über den Betrieb bis hin zu den einzelnen Schutzmechanismen.

Die folgenden Abschnitte zeigen im Detail, wie die Plattform Bedrohungen abwehrt, Compliance-Vorgaben erfüllt und gleichzeitig volle Kontrolle über Daten und Infrastruktur gewährleistet.

Architektur und Sicherheitsmodell von OpenCloud

OpenCloud ist von Grund auf so konzipiert, dass Sicherheit, Transparenz und volle Datenkontrolle im Mittelpunkt stehen. Die Plattform setzt auf eine moderne Drei-Schichten-Architektur (Three-Tier Architecture) und kombiniert bewährte Cloud-native-Prinzipien mit gezielten Designentscheidungen, um die Angriffsfläche zu minimieren und den Betrieb zu vereinfachen.

Drei Schichten für maximale Kontrolle

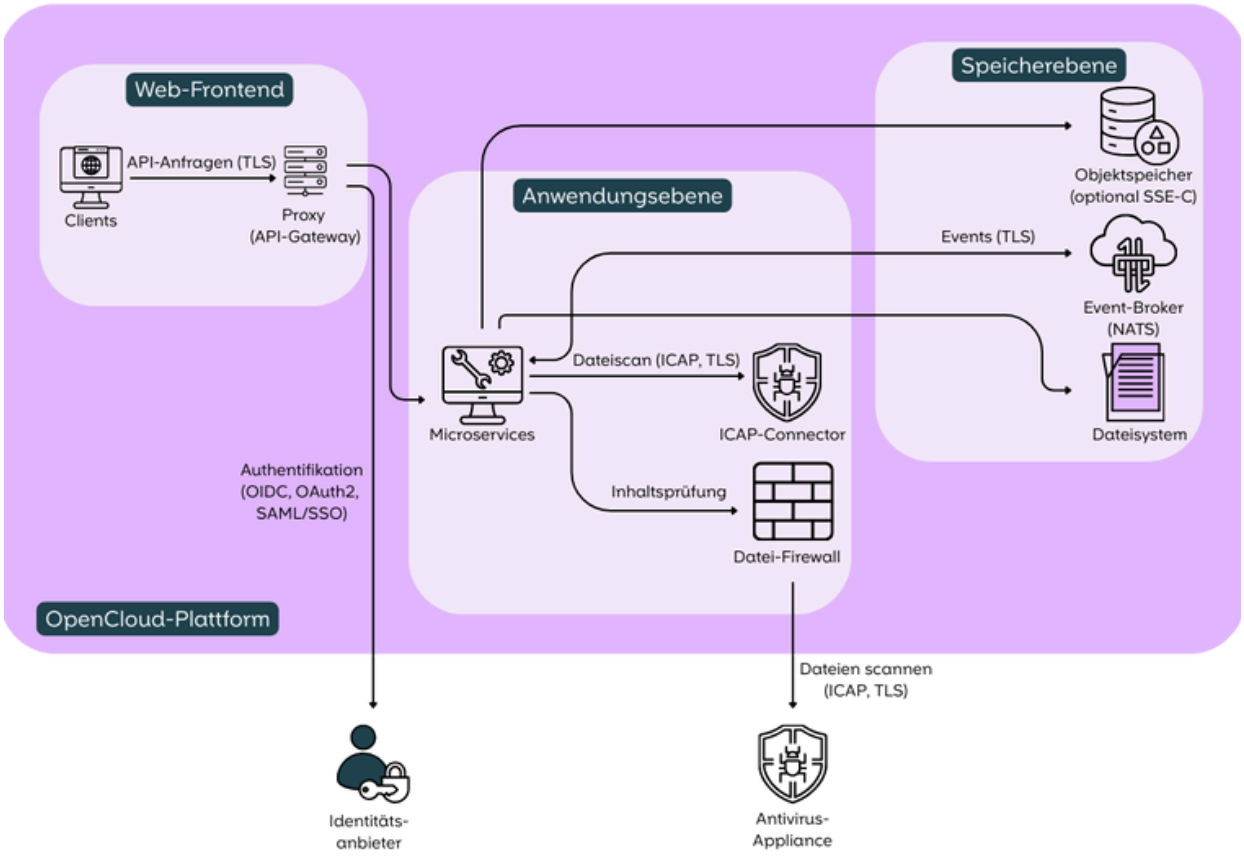
OpenCloud trennt Web-Frontend, Anwendungsschicht und Speicherebene strikt voneinander. Alle Anfragen laufen zunächst über einen vorgeschalteten Proxy, der als API-Gateway nur autorisierte Zugriffe zulässt. Die Anwendungsschicht besteht aus modularen Microservices, die über sichere TLS-Verbindungen mit weiteren Diensten kommunizieren.

Die Speicherebene verwaltet alle Dateien und Metadaten. Hier kommen ein angebundener Objektspeicher (optional mit SSE-C-Verschlüsselung), das Dateisystem sowie der Event-Broker NATS zum Einsatz. NATS übernimmt den sicheren, TLS-verschlüsselten Nachrichtenaustausch zwischen Anwendung und Speicher.

Dieses Design sorgt für klare Zuständigkeiten und verhindert, dass sich Angriffe oder Fehler seitlich im System ausbreiten. OpenCloud verschlüsselt alle Verbindungen zwischen Diensten und Schichten konsequent mit TLS – intern wie extern.

Architektur und Sicherheitsmodell von OpenCloud

Sichere Architektur von OpenCloud



Kompilierter Code statt dynamischer Ausführung

OpenCloud verzichtet auf dynamisch interpretierte Sprachen wie PHP und setzt stattdessen auf kompilierten Code, der ausschließlich in signierten Containern ausgeliefert wird. Änderungen am System erfordern einen Neubau und eine erneute Signatur.

Damit sind Manipulationen zur Laufzeit ausgeschlossen – ein wesentlicher Unterschied zu klassischen Webanwendungen, die Quellcode direkt interpretieren. Durch den verbindlichen Build- und Signaturprozess wird die Angriffsfläche deutlich reduziert, da keine externen Skripte oder Module spontan ins System eingebracht werden können.

Architektur und Sicherheitsmodell von OpenCloud

Datenhaltung ohne Datenbank

OpenCloud speichert alle Metadaten direkt im Dateisystem oder in einem angebundenen Objektspeicher. Eine (SQL-)Datenbank ist daher nicht erforderlich – Angriffsvektoren wie SQL-Injection entfallen so.

Gleichzeitig lässt sich die Plattform einfacher sichern: Da OpenCloud auf eine Datenbank verzichtet, genügt ein Snapshot des Dateisystems oder Objektspeichers, um ein vollständiges Backup zu erzeugen.

Für besonders hohe Anforderungen kann OpenCloud so erweitert werden, dass auch clientseitige Verschlüsselung und die Nutzung eigener Schlüssel per SSE-C (Server-Side Encryption with Customer Keys) unterstützt werden. Damit wäre es möglich, dass Organisationen ihre Schlüssel vollständig in eigener Hand behalten.

Vertrauenswürdige Container durch Signaturen

Alle Container sind kryptografisch signiert. Beim Deployment prüft OpenCloud, ob ein Image authentisch und unverändert ist. So gelangen keine manipulierten oder aus unsicheren Quellen stammenden Container ins System.

Damit legt OpenCloud besonderes Augenmerk auf die Integrität der eingesetzten Software und stärkt die Sicherheit in der gesamten Lieferkette – vom Quellcode bis zur produktiven Umgebung.

Identitäts- und Berechtigungsmanagement

Wer mit sensiblen Daten arbeitet, braucht verlässliche Mechanismen zur Authentifizierung und Rechtevergabe. OpenCloud bringt dafür ein durchdachtes System mit, das sich flexibel in bestehende IT-Landschaften integrieren lässt – von der Anmeldung bis zur Zugriffskontrolle.

Starke Authentifizierung & Rechtevergabe

Alle Programmierschnittstellen (APIs) von OpenCloud sind abgesichert. Die Plattform setzt auf moderne Authentifizierungs-Mechanismen und unterstützt offene Standards wie OpenID Connect (OIDC), OAuth 2.0 und Security Assertion Markup Language (SAML).

Damit lässt sich OpenCloud problemlos an vorhandene Identitätsdienste wie Keycloak, LDAP oder Active Directory anbinden – etwa für Single Sign-on (SSO) oder Zwei-Faktor-Authentifizierung.

Falls spezielle Anforderungen bestehen, lassen sich auch eigene Lösungen integrieren, etwa firmenspezifische Systeme, Token-Mechanismen, eigene Benutzerdatenbanken oder Hardware-basierte Authentifizierungen.

Organisationen behalten die volle Kontrolle über ihre zentrale Benutzerverwaltung und können bestehende Berechtigungskonzepte weiterführen.

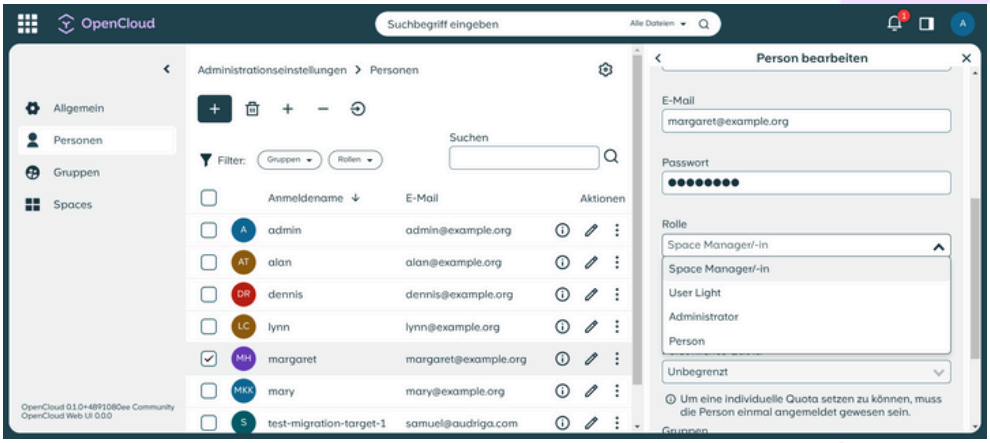


Abb.: OpenCoud Rechtevergabe an einzelne Person

Identitäts- und Berechtigungsmanagement

Trennung von Rechten

OpenCloud folgt dem Prinzip der rollenbasierten Berechtigungstrennung („Separation of Duties“): Wer einen Arbeitsbereich (Space) erstellt, erhält nicht automatisch Zugriff auf den Inhalt. Leserechte, Schreibrechte und Verwaltung lassen sich unabhängig voneinander festlegen.

Das schützt sensible Daten davor, versehentlich offengelegt oder unbefugt verändert zu werden. Gleichzeitig behalten Administrator*innen und Verantwortliche jederzeit den Überblick darüber, wer worauf zugreifen kann – ein wichtiger Aspekt für Sicherheit und Nachvollziehbarkeit.

Flexible Betriebsmodelle

OpenCloud passt sich den Rahmenbedingungen vor Ort an – nicht umgekehrt. Ob im eigenen Rechenzentrum, in einer Private Cloud oder komplett isoliert im Air-Gap-Betrieb: OpenCloud lässt sich so betreiben, wie es die jeweiligen Compliance-Anforderungen vorgeben.

Die Kontrolle über Standort, Netzwerkzugang und Datenhaltung bleibt dabei vollständig bei der betreibenden Organisation. Kein externer Dienstleister und kein Anbieter aus Drittstaaten kann auf die Umgebung zugreifen. Das macht OpenCloud besonders attraktiv für Organisationen mit hohem Schutzbedarf – etwa im öffentlichen Sektor, in der Forschung oder in sicherheitskritischen Infrastrukturen.

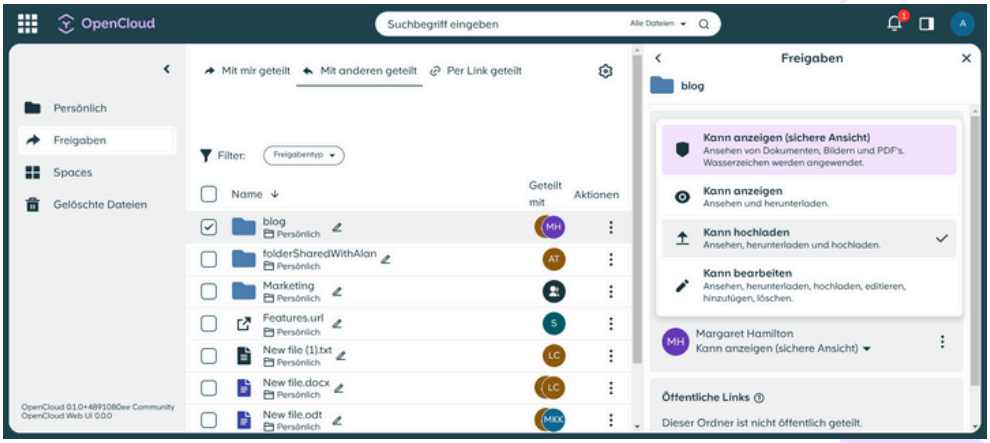


Abb.: OpenCoud Ansicht der Freigaben

Mehrschichtiger Schutz vor Malware

Datei-Uploads gehören zu den häufigsten Angriffspunkten in webbasierten Systemen. Schadsoftware, versteckte Skripte oder getarnte Dateiformate können schwerwiegende Folgen haben – vom Datendiebstahl bis zur vollständigen Kompromittierung der Plattform. OpenCloud begegnet dieser Bedrohung mit einem mehrschichtigen Schutzkonzept für hochgeladene Dateien.

Virenschutz auf Enterprise-Niveau

OpenCloud lässt sich direkt mit unternehmensweiten Virenschutz-Lösungen koppeln – über das ICAP-Protokoll (Internet Content Adaptation Protocol). Jeder Upload wird dabei in Echtzeit an ein externes Virenscanner-System übergeben, etwa an eine dedizierte Appliance oder eine in der Infrastruktur vorhandene Scan-Engine. Erst wenn die Datei als unbedenklich eingestuft wurde, nimmt OpenCloud sie ins System auf – andernfalls bleibt sie in Quarantäne und wird nicht über Shares verteilt.

So schützen Administrator*innen die Cloud vor Schadsoftware, Ransomware und anderen dateibasierten Angriffen – und erfüllen gleichzeitig zentrale Anforderungen an IT-Sicherheit und Compliance.

Inhaltsbasierte Dateiprüfung

Zusätzlich prüft OpenCloud auch die tatsächlichen Inhalte von Dateien – unabhängig von ihrer Dateiendung. Eine vermeintliche Bilddatei mit eingebettetem Schadcode fällt so auf, auch wenn sie korrekt benannt ist. Diese sogenannte File Firewall greift tief in die Datenstruktur und erkennt Abweichungen zwischen deklarierter und tatsächlicher Dateiform.

Zentrale Sicherheitsfunktionen von OpenCloud

Funktion	Beschreibung
API-Authentifizierung	Alle Schnittstellen sind mit starker Authentifizierung abgesichert (OIDC, OAuth2, SAML).
Trennung von Berechtigungen	Rechte für Erstellung und Zugriff auf Arbeitsbereiche (Spaces) sind unabhängig – kein automatischer Vollzugriff.
Kompilierter Code	Änderungen erfordern Kompilierung; verhindert Laufzeit-Manipulationen und Code Injection.
Drei-Schichten-Architektur	Web, Anwendung und Speicher sind strikt getrennt.
Virenschutz (ICAP-Integration)	Anbindung externer Virenscanner über ICAP zur Prüfung aller Uploads in Echtzeit.
Firewall für Dateiinhalte	Inhaltliche Überprüfung statt nur Dateierweiterungen.
Signierte Container	Nur kryptografisch geprüfte Images werden ausgeführt; schützt vor Supply-Chain-Angriffen.
Keine Datenbank	Alle Daten liegen direkt im Dateisystem; das reduziert mögliche Angriffspunkte.
TLS-Verschlüsselung	Sämtliche Verbindungen sind vollständig TLS-verschlüsselt – intern wie extern.
SSE-C & clientseitige Verschlüsselung	Vertrauliche Daten lassen sich mit eigenen Schlüsseln verschlüsseln und bereits vor dem Upload sichern.
Kontrolle über den Betrieb	Betrieb on-premises, in der Private Cloud oder vollständig isoliert (Air-Gap).

Vorteile gegenüber PHP-basierten Lösungen

Viele klassische File-Management-Systeme basieren auf PHP – einer weit verbreiteten, aber dynamisch interpretierten Skriptsprache. OpenCloud geht hier bewusst einen anderen Weg.

Die Plattform basiert auf kompiliertem Code, der als signierter Container ausgeliefert wird. Das bringt gleich mehrere Sicherheits- und Stabilitätsvorteile mit sich.

1. **Weniger Angriffsfläche, klar geregelte Abhängigkeiten:** Keine dynamische Code-Ausführung, weniger Schwachstellen – Abhängigkeiten werden im Entwicklungsprozess geprüft und abgesichert.

2. **Keine Code Injection durch dynamische Skript-Ausführung:** Kompilierter Code lässt sich zur Laufzeit nicht manipulieren. Einschleusen von Schadcode über Formulare, POST-Requests oder eval()-Funktionen ist technisch ausgeschlossen.

3. **Mehr Stabilität und planbare Performance:** OpenCloud läuft unabhängig von Hostsystemen oder PHP-Modulen, sondern in signierten, isolierten Container-Umgebungen. Das reduziert Seiteneffekte und sorgt für konstante Performance – auch bei Updates oder hoher Last.

Compliance und digitale Souveränität mit OpenCloud

OpenCloud unterstützt Organisationen dabei, regulatorische Vorgaben zu erfüllen und gleichzeitig die Hoheit über ihre Daten zu behalten – unabhängig von Cloud-Anbietern, Rechtsräumen oder proprietären Technologien.

OpenCloud erfüllt die Anforderungen der DSGVO und lässt sich an branchenspezifische Regelwerke wie den BSI-Grundschutz oder KRITIS-Vorgaben anpassen. Funktionen wie Protokollierung, transparente Rechtevergabe und flexible Speicherorte unterstützen eine datenschutzkonforme Nutzung.

Alle Daten bleiben vollständig unter Ihrer Kontrolle – unabhängig davon, ob Sie OpenCloud im eigenen Rechenzentrum, in einer Private Cloud oder in einer vollständig abgeschotteten Umgebung (Air-Gap) betreiben. Externe Dienstleister oder Drittstaaten haben keinen Zugriff.

Durch offene Standards, quelloffene Komponenten und eine klare Architektur ist OpenCloud auditierbar und langfristig wartbar. Die Plattform ist mandantenfähig und lässt sich in föderalen oder komplexen IT-Strukturen problemlos integrieren.

OpenCloud ist damit nicht nur technisch sicher, sondern schafft auch die Voraussetzung für digitale Unabhängigkeit im Sinne einer echten souveränen IT-Infrastruktur.

Ihre Entscheidung für digitale Souveränität

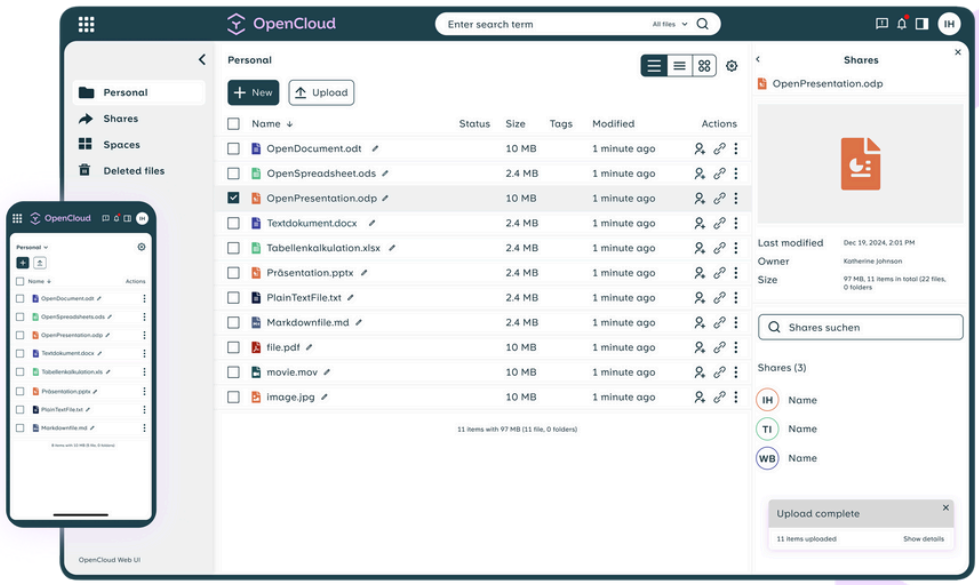
OpenCloud bietet eine sichere, auditierbare Plattform für Datei-Management, Datei-Sharing und digitale Zusammenarbeit – entwickelt für Organisationen mit höchsten Anforderungen an Datenschutz, Kontrolle und Flexibilität.

Die Kombination aus kompiliertem Code, geprüften Containern, flexiblen Berechtigungskonzepten und vollständiger Datenhoheit macht Open-Cloud zu einer zukunftssicheren Plattform. Von der sicheren Architektur bis zur Unterstützung von Air-Gap-Umgebungen erfüllt OpenCloud alle Voraussetzungen für einen souveränen, DSGVO-konformen IT-Betrieb.

Setzen Sie auf Open Source, offene Standards und volle Kontrolle – und entscheiden Sie sich für eine Plattform, die zu Ihrer Sicherheitsstrategie passt.

Schützen Sie Ihre Daten mit einer Plattform, die von Grund auf für maximale Sicherheit entwickelt wurde. Sprechen Sie mit uns über Ihre Sicherheitsstrategie – wir zeigen Ihnen, wie OpenCloud sich nahtlos in Ihre Infrastruktur integrieren lässt.

Kontaktieren Sie uns gern unter sales@opencloud.eu.
Wir freuen uns auf Ihre Anfrage.



OpenCloud

https://opencloud.eu