



DATEN, DIE NIEMAND EINSEHEN KANN NICHT EINMAL DER BETREIBER SELBST

DRIVELOCK IDGARD | POWERED BY SEALED CLOUD

SEALED CLOUD

Cloud-Daten sind heute gut geschützt – solange sie ruhen oder übertragen werden. Sobald sie verarbeitet werden, liegen sie jedoch unverschlüsselt im Arbeitsspeicher – erreichbar für jeden mit ausreichenden Administratorrechten, sei es beim Cloud-Anbieter, bei einem Insider oder durch behördlichen Zugriff. Sealed Cloud schließt genau diese Lücke.

1.200+

Unternehmen vertrauen bereits auf idgard

200.000+

aktive Nutzer im produktiven Einsatz

ISO 27001

+ ISO 9001 zertifiziert (idgard GmbH)

DAS PROBLEM: DATEN IN NUTZUNG SIND UNGESCHÜTZT

Verschlüsselung schützt Daten im Ruhezustand und bei der Übertragung. Sobald eine Anwendung mit den Daten arbeitet, müssen sie jedoch entschlüsselt vorliegen – im Arbeitsspeicher, sichtbar für jeden mit privilegiertem Systemzugriff.

Genau hier setzen Datenschutzverletzungen, Insider-Vorfälle und behördliche Zugriffe an, unabhängig vom Cloud-Anbieter.

DIE LÖSUNG: OPERATOR SHIELDING

Sealed Cloud ist die technische Architektur hinter DriveLock idgard: Sie schließt den Betreiber selbst technisch von jedem Zugriff auf Kundendaten aus – nicht nur vertraglich, sondern durch die Kombination aus physischer Isolation, kryptografischer Absicherung und automatisierten Kontrollprozessen.

IHRE VORTEILE AUF EINEN BLICK

Technisches statt vertragliches Vertrauen:

Klassische Cloud-Verträge (AVV, SLA, Zertifizierung) verbieten dem Betreiber den Zugriff – Sealed Cloud macht ihn technisch unmöglich. Das lässt sich gegenüber Prüfern, Aufsichtsbehörden und Kunden als Architekturnachweis belegen, nicht nur als Papierversprechen.

Schutz vor extraterritorialem Zugriff:

Durchgängig deutsche/europäische Rechtskette – Unternehmenssitz, Rechenzentrum, Personal, Verträge – reduziert die Angriffsfläche durch den US CLOUD Act oder vergleichbare außereuropäische Zugriffsansprüche.

Regulatorische Anforderungen direkt adressiert:

Sealed Cloud unterstützt zentrale Vorgaben von NIS2 (IT-Souveränität für KRITIS-Betreiber), DORA (geringeres IKT-Drittparteienrisiko), DSGVO Art. 25/32 (Privacy/Security by Design) und dem EU AI Act (souveräne Infrastruktur für hochriskante KI-Systeme) – durch Architektur nachweisbar, nicht nur durch Prozessdokumentation.

Flexibel einsetzbar über mehrere Betriebsformen:

Ob als fertige Anwendung (Sealed SaaS, wie idgard), dediziertes Private-Cloud-as-a-Service-Angebot, souveränes Managed-Cloud-Hosting, On-Premise im eigenen Rechenzentrum oder als kompakte Edge-Instanz – das Architekturprinzip passt sich Ihrem Betriebsmodell an.

Klare Differenzierung gegenüber Hyperscalern:

Im Unterschied zu US-Hyperscalern (Root-Zugriff des Betreibers, US-Jurisdiktion) und zu „souveränen“ Angeboten, die im Kern nur delegierten Zugriff auf ausländische Infrastruktur umverpacken, kann Sealed Cloud den fehlenden Betreiberzugriff technisch belegen statt nur vertraglich zusichern.

Volle Anwendungskompatibilität:

Im Gegensatz zu klassischem Confidential Computing (SGX/SEV) ohne Spezialhardware, ohne Einschränkung bei GPU-Nutzung und mit planbarer Performance.

ZWEI WEGE, SEALED CLOUD ZU NUTZEN

Sealed Cloud ist keine einzelne Firma oder ein einzelnes Produkt, sondern ein Architekturprinzip. DriveLock idgard bringt es Ihnen fertig als Anwendung – oder Sie bauen darauf Ihre eigene Infrastruktur.

idgard – Sealed SaaS

Sofort einsatzbereit, produktiv im Einsatz bei über 1.200 Unternehmen

- › Fertige Lösung für sicheren Dateiaustausch und Zusammenarbeit (Enterprise Drive, idgard Box)
- › Betrieben von idgard GmbH, einer 100%igen Tochter der DriveLock SE
- › ISO 27001- und ISO 9001-zertifiziert, weitere Zertifizierungen in Vorbereitung (u. a. BSI C5, TISAX)
- › Referenzen u. a. Oldenburgische Landesbank, regio iT, Baker Tilly, CURACON
- › Abrechnung nutzerbasiert, kein Infrastruktur-Aufwand auf Kundenseite

Sealed Cloud Repository Subscription

Für Unternehmen, die eine eigene Sealed-Cloud-Infrastruktur betreiben möchten

- › Zugriff auf ein gepflegtes Repository mit Quellcode, Installations-/Steuerungsskripten und gehärteten Images
- › Sie bauen und betreiben Ihre eigene Sealed-Cloud-Instanz – wir pflegen und aktualisieren die Basis
- › Laufender Support sowie technische Begleitung (Onboarding, Technical Account Management) inklusive
- › Ideal für eigene Anwendungen, die von echtem Betreiberausschluss profitieren sollen
- › Modell aktuell in Vorbereitung – sprechen Sie uns für Details und Pilotprojekte an

WARUM NICHT KLASSISCHES CONFIDENTIAL COMPUTING?

Hardwarebasierte Enklaven (Intel SGX/TDX, AMD SEV-SNP) sind ein valider, aber begrenzter Ansatz: Sie erfordern spezielle Prozessoren, schränken die Anwendungskompatibilität ein und haben wiederholt Seitenkanal-Schwachstellen gezeigt. Sealed Cloud verfolgt einen komplementären, aber unabhängigen Weg über Server-Isolation statt Hardware-Vertrauen – ohne diese Einschränkungen.

SPRECHEN SIE MIT UNS

Ob fertige SaaS-Lösung oder eigene Infrastruktur:
Wir zeigen Ihnen, wie Sealed Cloud Ihre Daten auch dort schützt,
wo klassische Verschlüsselung an ihre Grenzen stößt.

www.idgard.com · sales@idgard.com

ÜBERZEUGEN SIE SICH

Jetzt gratis und
unverbindlich testen.



idgard GmbH
Landsberger Straße 396
81241 München

+49 (89) 546 36 49-0

Drivelock idgard ist eine
Subbrand der DriveLock SE

