



DATA THAT NO ONE CAN ACCESS NOT EVEN THE OPERATOR ITSELF

DRIVELOCK IDGARD | POWERED BY SEALED CLOUD

SEALED CLOUD

Cloud data is well protected today, as long as it is at rest or in transit. However, the moment data is processed, it must be decrypted in memory, making it accessible to anyone with sufficient administrative privileges, whether at the cloud provider, through an insider threat, or via government access requests. Sealed Cloud closes precisely this gap.

1.200+

Companies already trust idgard

200.000+

Active users in productive operation

ISO 27001

+ ISO 9001 certified (idgard GmbH)

THE PROBLEM: DATA IN USE IS UNPROTECTED

Encryption protects data at rest and in transit. However, whenever an application processes data, it must exist in decrypted form in memory, visible to anyone with privileged system access.

This is exactly where data breaches, insider incidents, and government access requests occur, regardless of the cloud provider.

THE SOLUTION: OPERATOR SHIELDING

Sealed Cloud is the underlying technology architecture behind idgard. It technically prevents even the operator itself from accessing customer data, not merely through contractual agreements, but through a combination of physical isolation, cryptographic safeguards, and automated control mechanisms.

YOUR BENEFITS AT A GLANCE

Technical trust instead of contractual trust:

Traditional cloud agreements (DPAs, SLAs, certifications) prohibit operators from accessing data. Sealed Cloud makes such access technically impossible. This can be demonstrated to auditors, regulators, and customers as an architectural proof, rather than relying solely on contractual assurances.

Protection against extraterritorial access:

A fully German and European legal chain consisting of company headquarters, data centers, personnel, and contractual relationships reduces exposure to the US CLOUD Act and similar non-European access claims.

Directly addresses regulatory requirements:

Sealed Cloud supports key requirements of NIS2 (IT sovereignty for critical infrastructure operators), DORA (reduced ICT third-party risk), GDPR Articles 25 and 32 (Privacy and Security by Design), and the EU AI Act (sovereign infrastructure for high-risk AI systems). Compliance is supported through architecture and technical design, not merely through process documentation.

Flexible deployment models:

Whether as a ready-to-use application (Sealed SaaS, such as idgard), a dedicated Private Cloud as a Service offering, sovereign managed cloud hosting, an on-premises deployment within your own data center, or a compact edge instance, the architectural principle adapts to your operating model.

Clear differentiation from hyperscalers:

Unlike US hyperscalers, where operators retain root-level access and fall under US jurisdiction, and unlike many „sovereign cloud“ offerings that essentially repackage delegated access to foreign infrastructure, Sealed Cloud can technically prove operator exclusion rather than merely contractually promise it.

Full application compatibility:

Unlike traditional confidential computing approaches (SGX/SEV), Sealed Cloud requires no specialized hardware, imposes no restrictions on GPU usage, and delivers predictable performance.

TWO WAYS TO USE SEALED CLOUD

Sealed Cloud is not a single company or product. It is an architectural principle. idgard delivers it as a ready-to-use application, or you can use it as the foundation for your own infrastructure.

idgard – Sealed SaaS

Complete solution for secure file sharing and collaboration (Company Drive, idgard Box)

- Operated by idgard GmbH, a wholly owned subsidiary of DriveLock SE
- ISO 27001 and ISO 9001 certified, with additional certifications in preparation (including BSI C5 and TISAX)
- Trusted by organizations such as Oldenburgische Landesbank, regio iT, Baker Tilly, and CURACON
- User-based pricing model with no infrastructure effort required on the customer side

Sealed Cloud Repository Subscription

For organizations that want to operate their own Sealed Cloud infrastructure.

- Access to a maintained repository including source code, installation and orchestration scripts, and hardened images
- You build and operate your own Sealed Cloud environment while we maintain and update the underlying platform
- Ongoing support and technical guidance, including onboarding and Technical Account Management
- Ideal for proprietary applications that should benefit from true operator exclusion
- Offering currently in preparation. Contact us for details and pilot project opportunities

WHY NOT TRADITIONAL CONFIDENTIAL COMPUTING?

Hardware-based enclaves such as Intel SGX/TDX and AMD SEV-SNP represent a valid but inherently limited approach. They require specialized processors, can restrict application compatibility, and have repeatedly been affected by side-channel vulnerabilities. Sealed Cloud follows a complementary yet independent path, relying on server isolation rather than hardware trust, while avoiding these limitations.

TALK TO US

Whether you are looking for a ready-to-use SaaS solution or your own sovereign infrastructure, we can show you how Sealed Cloud protects your data even where traditional encryption reaches its limits.

www.idgard.com · sales@idgard.com

LEARN MORE

Try it now for free and
with no obligation.



idgard GmbH
Landsberger Straße 396
81241 Munich

+49 (89) 546 36 49-0

Drivelock idgard is a
Subbrand of DriveLock SE



ISO/IEC 27001
Certified Information Security
Management System
www.tuvsud.com/ms-cert