

# AGENTIC AI CONTROL

idgard – der sichere Gatekeeper  
für Ihre Daten im AI-Zeitalter.

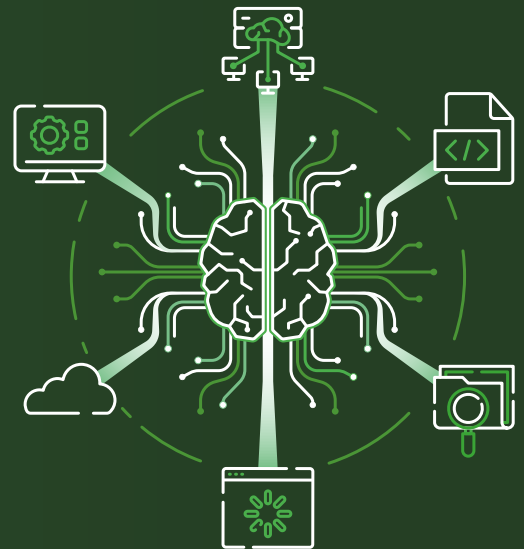


# Wenn KI-Agenten auf Ihre Daten zugreifen

Autonome KI-Agenten verändern die Art, wie Daten genutzt werden – aber auch, wie sie gefährdet sind.

## Unsichtbare Risiken

KI-Agenten greifen grundsätzlich auf alle Datenquellen zu, die ihnen verfügbar sind. Besonders kritisch wird dies bei lokal auf Endgeräten gespeicherten Daten, da diese für die KI leicht zugänglich sind. Ohne gezielte Schutzmaßnahmen bedeutet das: Sämtliche lokal vorhandenen Informationen können von KI-Agenten vollständig eingesehen und genutzt werden.



## Warum das **problematisch** ist

**KI-Agenten handeln nicht immer kontrolliert:**

- › durch fehlerhafte Entscheidungen
- › durch manipulierte oder irreführende Informationen im Internet
- › durch fehlende Sicherheitsmechanismen
- › oder schlicht durch unbeabsichtigte Fehler

## Konsequenzen für Ihr Unternehmen

- › Datenleaks an externe AI-Services
- › Verlust vertraulicher Informationen durch Nutzung in Trainingsdaten
- › Unbemerkte Datenveränderungen – absichtlich oder versehentlich

Kurz gesagt:

*Wo Daten ungeschützt  
verfügbar sind, sind sie auch für  
KI-Agenten verfügbar.*

# idgard: Sicherer Zugriff statt unkontrollierter KI

idgard schützt Ihre Daten konsequent – auch vor autonomen KI-Agenten.

## Ihre Sicherheitsvorteile

- › Keine lokale Datenspeicherung als Standard
- › Kein Zugriff durch KI-Agenten ohne Freigabe
- › Vollständige Kontrolle über Datenzugriffe

Wenn KI gezielt eingesetzt wird

**Sie entscheiden bewusst, wann und wie KI auf Daten zugreifen darf:**

- › Granulare Zugriffskontrolle (ERM)
- › KI sieht nur Daten, die ausdrücklich freigegeben sind
- › Lückenlose Nachvollziehbarkeit
- › Zugriff und Änderungen jederzeit auditierbar
- › Kryptografisch abgesichert

## Zwei sichere Einsatzszenarien

### 1. KI-Agent mit kontrolliertem Zugriff

- › Eigener Benutzer für den Agenten
- › Zugriff über API – kein Zusatzsystem notwendig
- › Vollständig steuerbar & nachvollziehbar

#### Ideal für:

Automatisierung, Analyse, sichere AI-Integration

### 2. KI-Agent mit lokalem Zugriff

- › Nur gezielt heruntergeladene Daten werden genutzt
- › Keine Einsicht in andere Inhalte
- › Volle Kontrolle bleibt beim Nutzer

#### Ideal für:

Einzelaufgaben, maximale Datensicherheit

## Praxisbeispiel

### Ohne idgard:

Die KI verarbeitet lokale Dateien, wodurch vertrauliche Dokumente unbeabsichtigt mit übermittelt werden können. In der Folge gelangen diese Daten möglicherweise in die Trainingssysteme externer AI-Dienste. Zusätzlich besteht das Risiko, dass manipulierte Inhalte in die Verarbeitung einfließen und so zu verfälschten oder falschen Ergebnissen führen.

### Mit idgard:

Es werden ausschließlich die tatsächlich benötigten Daten freigegeben, wodurch unbemerkte Zugriffe verhindert werden. Gleichzeitig bleibt jede Aktivität transparent, da Änderungen jederzeit nachvollziehbar sind. Auf diese Weise bleiben vertrauliche Inhalte durchgehend geschützt.

# Fazit

**Autonome KI braucht Kontrolle. idgard ist Ihr Schutzschild:**

- › Sie bestimmen, was KI sehen darf
- › Sie verhindern Datenleaks zuverlässig
- › Sie behalten jederzeit die Kontrolle



# We create trust through security.

idgard GmbH  
Landsberger Str. 396  
81241 München

+49 (0)89-444 435 140  
contact@idgard.com  
www.idgard.com

idgard vereint hochsicheren Datenaustausch und virtuelle Datenräume in einem Produkt – für eine effiziente und rechtskonforme digitale Zusammenarbeit. Höchste Sicherheits- und Compliance-Anforderungen werden erfüllt, wodurch eine DSGVO-konforme Verarbeitung sensibler Daten gewährleistet ist.

Mehr als 1.200 Unternehmen vertrauen bereits auf idgard, darunter IT- und Kommunikationsanbieter, Unternehmensberatungen, Finanzdienstleister, Behörden und Betreiber kritischer Infrastrukturen.

