

GOVERNED ACCESS LAYER

# COLOSSOS

**Sicherer Einsatz agentischer KI auf bestehenden Enterprise-Systemen — ohne Replatforming.**

Governance, Compliance, IT-Security und Investitionssicherheit für Agentische KI im Enterprise-Kontext.



Enterprise Systeme

**COLOSSOS  
Governed  
Access Layer**

Agentische KI-  
Bearbeitung

*Der sichere Weg zum Einsatz agentischer KI*

# Die eigentliche Enterprise-Lücke

Standardprozesse sind digitalisiert. Die kostenintensiven und komplexen Ausnahmefälle bleiben menschlich koordiniert.

DIGITALISIERT

## Standardprozesse

- › Self-Service
- › i.d.R. eins bis wenige Systeme betroffen
- › klare Prozesspfade



HÄNGT FEST

## Ausnahmefälle

- › unvollständige Fälle
- › Status- und Datenkonflikte
- › Freigaben und Eskalationen



KOSTENBLOCK

## Casework

- › manuelle Bearbeitung notwendig
- › mehrere Systeme betroffen
- › manuelle Kontextbildung
- › hohe Governance-Anforderung

# Warum agentische KI aktuell noch nicht produktiv skaliert

Die Technik ist da. Die kontrollierte Ausführung auf Enterprise-Systemen fehlt.

1

## RPA

stark bei stabilen Regeln

---

**bricht bei Ausnahmen  
und Komplexität**

2

## Copiloten

helfen Menschen

---

**führen nicht  
eigenständig aus**

3

## API / Middleware

verbindet Systeme

---

**keine Compliance,  
kein Audit-Log**

4

## KI-Plattformen

bringen Agenten

---

**binden Kompetenzen  
an eigene Plattformen**

**Die Lücke ist nicht „noch mehr KI“, sondern ein sicherer Operating Layer  
zwischen Agenten und bestehenden Systemen.**

# COLOSSOS schließt die Lücke

Ein Governed Access Layer für sichere agentische KI-Ausführung auf bestehenden Enterprise-Systemen.



**Ohne Replatforming: COLOSSOS kontrolliert den Pfad von KI-Einsatz → Fallkontext & Aktionen → Auditierbarkeit.**

# Sicherheit hat drei operative Dimensionen

COLOSSOS macht agentische Ausführung rechtssicher und compliant möglich.

1

## Compliance

Nachvollziehbarkeit, Policy-Anwendung und Audit-Trail für prüfbaren KI-Einsatz.

2

## Governance

Hoheit über erlaubte Aktionen, Freigaben, Skills und IT-Nutzung bleibt im Unternehmen.

3

## IT-Security

Kontrollierter Datenfluss: Agenten arbeiten nur mit freigegebenem Kontext und definierten Systemzugriffen.

**Der Kernnutzen: Agentische KI wird vom Risikoexperiment zum kontrollierbaren Enterprise-Betriebsmodell.**

# Investitionssicherheit in einem offenen Agentenmarkt

Welche Agentenplattform gewinnt, ist noch ungeklärt. Die wertvolle Prozessintelligenz sollte nicht dort gebunden sein.

## OHNE COLOSSOS

Skills + Workflows + Enterprise-Konnektoren  
liegen in der Agentenplattform

---

Plattformwechsel = Rebuild-Risiko

## MIT COLOSSOS

Skills + Workflows + Enterprise-Konnektoren  
verbleiben in COLOSSOS

Agentenschicht wird austauschbar

OpenAI

Anthropic

Agent X

Die Investition verbleibt in COLOSSOS — nicht in einer möglicherweise kurzlebigen Agentenplattform.

# Vom manuellen Casework zur kontrollierten Ausführung

COLOSSOS operationalisiert Ausnahmefälle für KI-Agenten — ohne bestehende Systeme zu ersetzen.

## HEUTE

### Mensch sammelt Kontext

aus mehreren Systemen

### Mensch interpretiert Fall

Daten, Regeln, Status

### Mensch entscheidet / eskaliert

mit Risiko und Wartezeit

## MIT COLOSSOS

### Fallkontext wird strukturiert

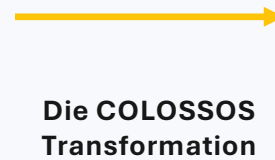
agent-consumable case context, skills & workflows

### Policies + Approvals steuern

erlaubte Actions und Freigaben, Human in the Loop

### Rechtssichere kontrollierte Ausführung

mit Audit-Logging und Review



**Werthebel: Weniger manuelle Koordination, schnellere Bearbeitung, bessere Kontrolle.**

# Was COLOSSOS im Unternehmen verankert

Zwei Kompetenzblöcke, die unabhängig vom jeweiligen Agentenmodell Wert schaffen.

## BLOCK 1

### Governance, Security & Audit Control

- › Policy Enforcement
- › Approval Gates
- › Data Security & Audit Trail

## BLOCK 2

### Skill- & Workflow- Management

- › Business Actions & Policies
- › Exception Workflows
- › Agent-consumable Case Context

**Gemeinsam entsteht ein kontrollierter Ausführungspfad für agentische KI — nicht nur eine technische Integration.**

# Der Einstieg: COLOSSOS Exception Casework Pilot

Ein klar begrenzter Pilot, der Wert und Lieferbarkeit beweist — ohne Plattformprojekt.

## SCOPE

- › 1 Ausnahmeprozess
- › 2–4 Systeme
- › 5–12 Business Actions
- › 1 Policy Pack
- › 1 Approval-Modell

## DELIVERY

- › 45 Tage Delivery-Zusage
- › nach Use-Case-Prüfung
- › deploybar, nicht deployed

## GUARDRAILS

- › keine Happy Paths
- › keine Replatforming-Story
- › keine generische Plattforminitiative
- › Scope-Änderungen nur nach Absprache

**Der Pilot soll einen realen Ausnahmeprozess agentisch bearbeitbar machen — sicher, auditierbar und auf bestehenden Systemen.**

# Warum jetzt?

Agentische KI ist die Realität und wird zukünftig zum entscheidenden Differentiator in einer effizienten unternehmerischen Kostenstruktur. Gewinnen wird, wer die Kontrolle über Ausführung und Daten behält und agentische KI schnell produktiv einführt und erfolgreich skaliert.

## Sichere Ausführung

Agenten greifen nur kontrolliert auf Kontext, Systeme, Daten und Actions zu.

## Keine Replatforming-Abhängigkeit

Bestehende Systeme bleiben. COLOSSOS ergänzt die Dimension des Governance- und Execution-Layers.

## Investitionsschutz

Skills und Workflows bleiben agentenagnostisch nutzbar.

## Beweisbarer Einstieg

Pilot fokussiert auf einen Ausnahmeprozess mit klarem Nutzen und transparenten Guardrails.

**Nächster Schritt: Einen geeigneten Anwendungsfall qualifizieren.**

GOVERNED ACCESS LAYER

# COLOSSOS

**Vielen Dank.**



COLOSSOS ist ein Produkt der ALLEHERZEN GmbH

Alwinenstr. 3 | 65189 Wiesbaden | Deutschland

[www.COLOSSOS.ai](http://www.COLOSSOS.ai) | [hello@COLOSSOS.ai](mailto:hello@COLOSSOS.ai)