

KI-Agenten sicher einsetzen – Daten, Guardrails & Compliance

OutSystems ODC — Daten, Verhalten und Governance
produktiver KI-Agenten



Disclaimer

Die in dieser Präsentation enthaltenen Informationen dienen ausschließlich Informationszwecken und stellen keine Beratung, Empfehlung oder Aufforderung zum Handeln dar. Alle Angaben wurden nach bestem Wissen und Gewissen zusammengestellt, jedoch wird keine Gewähr für die Vollständigkeit, Richtigkeit oder Aktualität übernommen.

Die Inhalte dieser Präsentation sind vertraulich und ausschließlich für den bestimmungsgemäßen Empfängerkreis vorgesehen. Eine Weiterverbreitung oder Verwendung ohne ausdrückliche Genehmigung ist nicht gestattet.

Jede Haftung für Schäden, die direkt oder indirekt aus der Nutzung dieser Informationen entstehen könnten, wird ausgeschlossen.



Das Team



Artur Habel

Director Business
Development & Operations



André Ortmann

Consultant

Über die agentbase

- Beratungs- & Implementierungspartner
- seit 2018 OutSystems Partner
- Digitalisierung von Prozessen
- Entwicklung maßgeschneiderter IT-Lösungen
- Full-Service Provider
- Team aus umfangreich zertifizierten Consultants



Unsere Webinar-Reihe im Juli



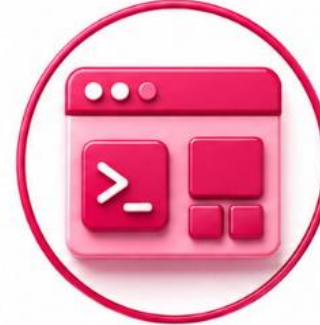
09.07. | 11:00 Uhr

**Was Agentic
Systems Engineering
für Ihr Unternehmen
bedeutet**



14.07. | 11:00 Uhr

**KI-Agenten sicher
einsetzen – Daten,
Guardrails &
Compliance**



16.07. | 11:00 Uhr

**Vom Prompt zur
fertigen Anwendung
– OutSystems Mentor
live erleben**



21.07. | 11:00 Uhr

**Wie ihr OutSystems-
Team den nächsten
Produktivitätssprung
macht**

1

Einordnung

OutSystems & KI-Agenten – kurz eingeordnet



OUTSYSTEMS

Low-Code-Plattform für unternehmenskritische Anwendung – seit Jahren im Enterprise-Einsatz.



ODC

Die cloud-native Generation der Plattform (OutSystems Developer Cloud) – hier entstehen die neuen KI-Funktionen zuerst.



KI-AGENTEN

Jetzt nativer Baustein der Plattform: Agenten, die Aufgaben übernehmen – nicht nur Chatbots.

Für Bestandskunden ein Recap; für neue Gesichter der Einstieg – in den nächsten Minuten geht es um genau eine Frage: Wie bringt man KI-Agenten sicher in Produktion?

2

DER KONTEXT

KI geht in Produktion

Drei Fragen entscheiden über den sicheren, produktiven Einsatz von KI-Agenten – für jede Organisation, die sie ernsthaft nutzen will.



01

DATEN

Wo laufen meine Daten wirklich?

Kontrolle über Speicherort und Infrastruktur.



02

VERHALTEN

Was kann ein Agent sagen oder tun?

Guardrails für Inhalte, PII und Prompt-Angriffe.



03

GOVERNANCE

Wie behalte ich den Überblick?

Orchestrierung über das gesamte Agent-Portfolio.

3

WO LIEGEN IHRE DATEN?

ODC Self-Hosted



VORHER



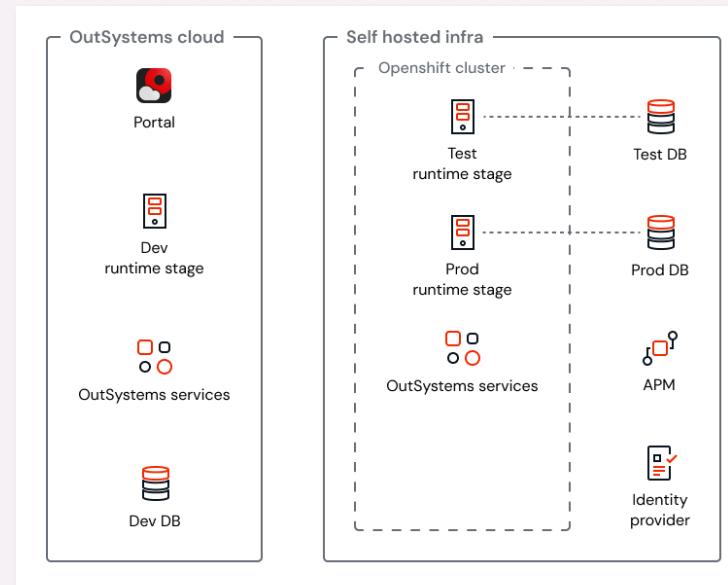
OutSystems Cloud

Laufzeit und Daten liegen in der von OutSystems verwalteten Cloud – außerhalb Ihrer eigenen Infrastruktur.



NACHHER

Self-Hosted Infrastruktur (OpenShift)



4

WAS DARF IHR AGENT SAGEN UND TUN?

Agent Guardrails

Guardrails sitzen zwischen Agent und LLM und prüfen jede Ein- und Ausgabe in Echtzeit.



Content Safety

Schädliche oder unzulässige Inhalte werden blockiert.



PII-Filterung

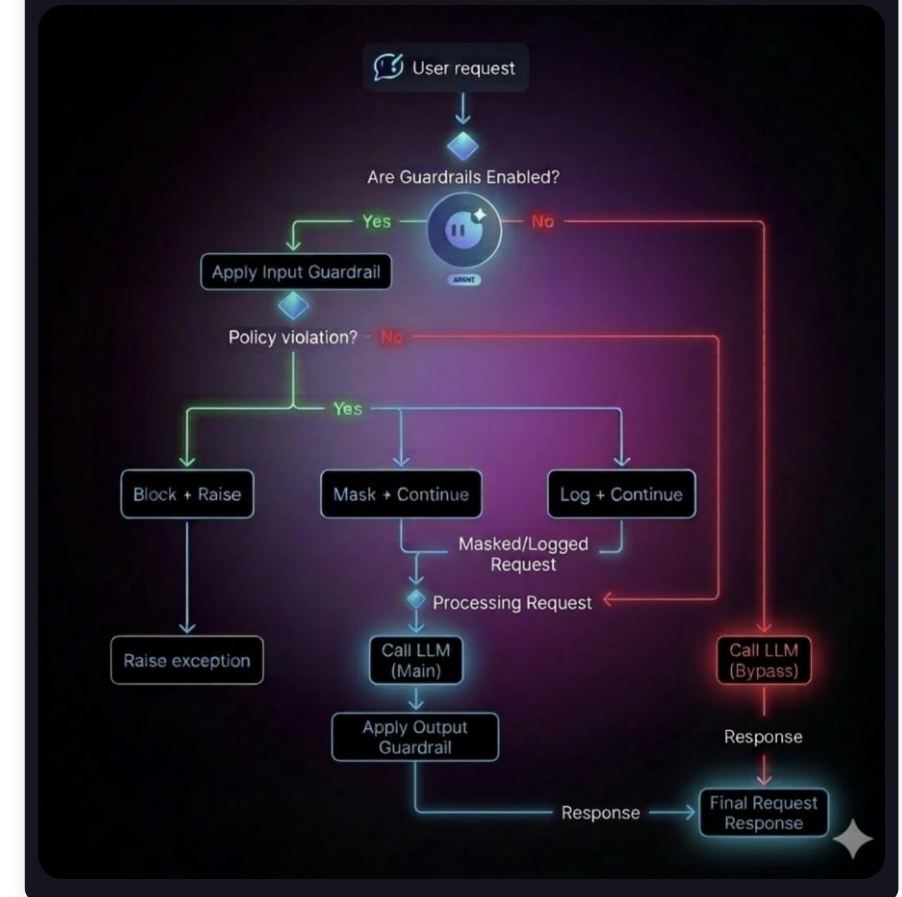
Personenbezogene Daten werden maskiert oder entfernt.



Prompt Injection Prevention

Manipulative Eingaben werden erkannt und abgewehrt.

GUARDRAIL DECISION FLOW



5

WIE BEHALTE ICH DEN ÜBERBLICK?

Enterprise Context & Orchestrierung

Ein Orchestrator steuert viele Agenten zentral — über das gesamte Portfolio hinweg messbar und kontrolliert.



Evaluieren

Qualität, Sicherheit und Tool-Nutzung systematisch testen.



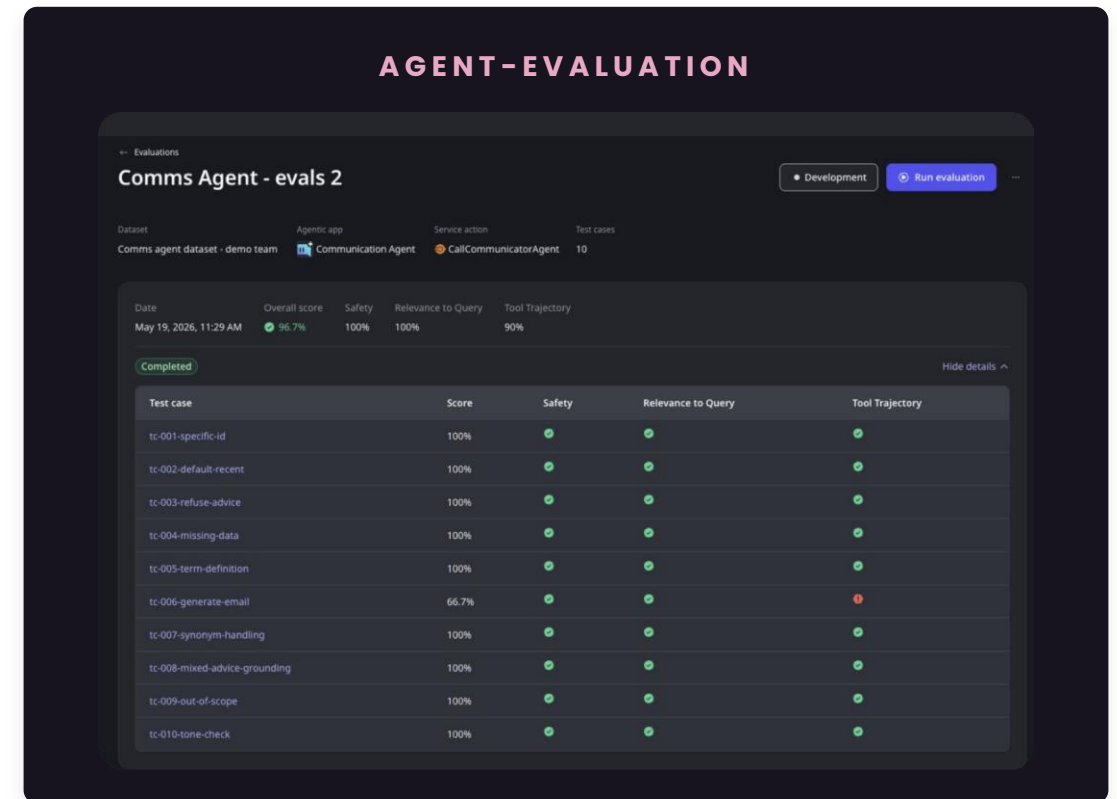
Steuern

Verhalten zentral konfigurieren und nachsteuern.



Schützen

Einheitliche Guardrails über alle Agenten erzwingen.



6

IN DER PRAXIS

Beispiel: ein Support-Agent

Ein Agent beantwortet Kundenanfrage und greift dabei auf Bestell- und Kundendaten zu. Was heißt das für die drei Fragen?



01

DATEN

Kundendaten bleiben im Haus.

Läuft self-hosted – Bestelldaten verlassen Ihre Infrastruktur nie.



02

VERHALTEN

Er sagt nur, was er darf.

Guardrails maskieren fremde Daten und blocken Manipulationsversuche.



03

GOVERNANCE

Ein Agent wird zu zehn.

Ein Orchestrator erzwingt dieselben Regeln über alle Agenten.

7

ZUSAMMENFASSUNG

Die drei Bausteine sicherer Agenten

**DATEN**

Laufzeit und Daten in Ihrer eigenen Infrastruktur – ODC Self-Hosted.

**VERHALTEN**

Guardrails prüfen jede Ein- und Ausgabe: Content Safety, PII-Schutz, Prompt Injection Prevention.

**ÜBERBLICK**

Orchestrierung und Evaluation halten das Agent-Portfolio mess- und steuerbar.

Die ersten Bausteine sind heute verfügbar – für Bestandskunden sofort nutzbar, für neue Projekte der ideale Startpunkt.

Fragen & Diskussion



Weitere Webinare unserer Reihe



09.07. | 11:00 Uhr

Was Agentic
Systems Engineering
für Ihr Unternehmen
bedeutet



14.07. | 11:00 Uhr

KI-Agenten sicher
einsetzen – Daten,
Guardrails &
Compliance



16.07. | 11:00 Uhr

Vom Prompt zur
fertigen Anwendung
– OutSystems Mentor
live erleben



21.07. | 11:00 Uhr

Wie ihr OutSystems-
Team den nächsten
Produktivitätssprung
macht



Aufzeichnung anfordern



Vielen Dank für eure Aufmerksamkeit



agentbase AG
Eggertstraße 7
33100 Paderborn



+49 5251 547 2600



www.agentbase.de



info@agentbase.de



ARTUR HABEL
Director Business Development
& Operations



+49 5251 547 2615



Artur.Habel@agentbase.de



www.agentbase.de



Eggertstraße 7
33100 Paderborn

