



EINSATZ // CIM LINGEN

# Mehr Team-Power mit KI: Agentensysteme für Microsoft 365 Copilot

Was trägt, wenn der Agent handelt statt antwortet?

**Nicole Enders**

Microsoft MVP seit 2020, 7× in Folge · Die Agentin

04.09.2026 · LINGEN · KI & DATEN



# Nicole Enders

Microsoft MVP seit 2020. Ich arbeite an der Schnittstelle zwischen dem, was technisch geht, und dem, was Menschen im Arbeitsalltag hilft.

## MISSION

***„Menschen und Organisationen mit intelligenten Lösungen verbinden, um zukunftssicher, produktiv und smarter zu arbeiten.“***

### ● Strategie

Klar. Zielgerichtet.

### ● Architektur

Sicher. Skalierbar.

### ● Umsetzung

Pragmatisch. Effizient.

### ● Adoption

Veränderung. Akzeptanz.

### ● Enablement

Wissen. Fähigkeiten.

### ● Impact

Erfolge. Mehrwert.





# Der Auftrag für die nächsten 40 Minuten.

01

## Die Lage

Warum dein Agenten-Wissen aus dem Frühjahr nicht mehr trägt.

02

## Das Prinzip

Harness, Wissen, Werkzeuge: woraus ein Agent heute besteht.

03

## Der Baukasten

Power Platform: finden, automatisieren, mit Kontext versorgen.

04

## Die Verteilung

Gebaut ist nicht verteilt. Was am Montag zu tun ist.



E I N S A T Z

# 01

## DIE LAGE

Im Juni 2026 wurde Copilot Studio neu gebaut. Das ändert mehr als die Oberfläche.

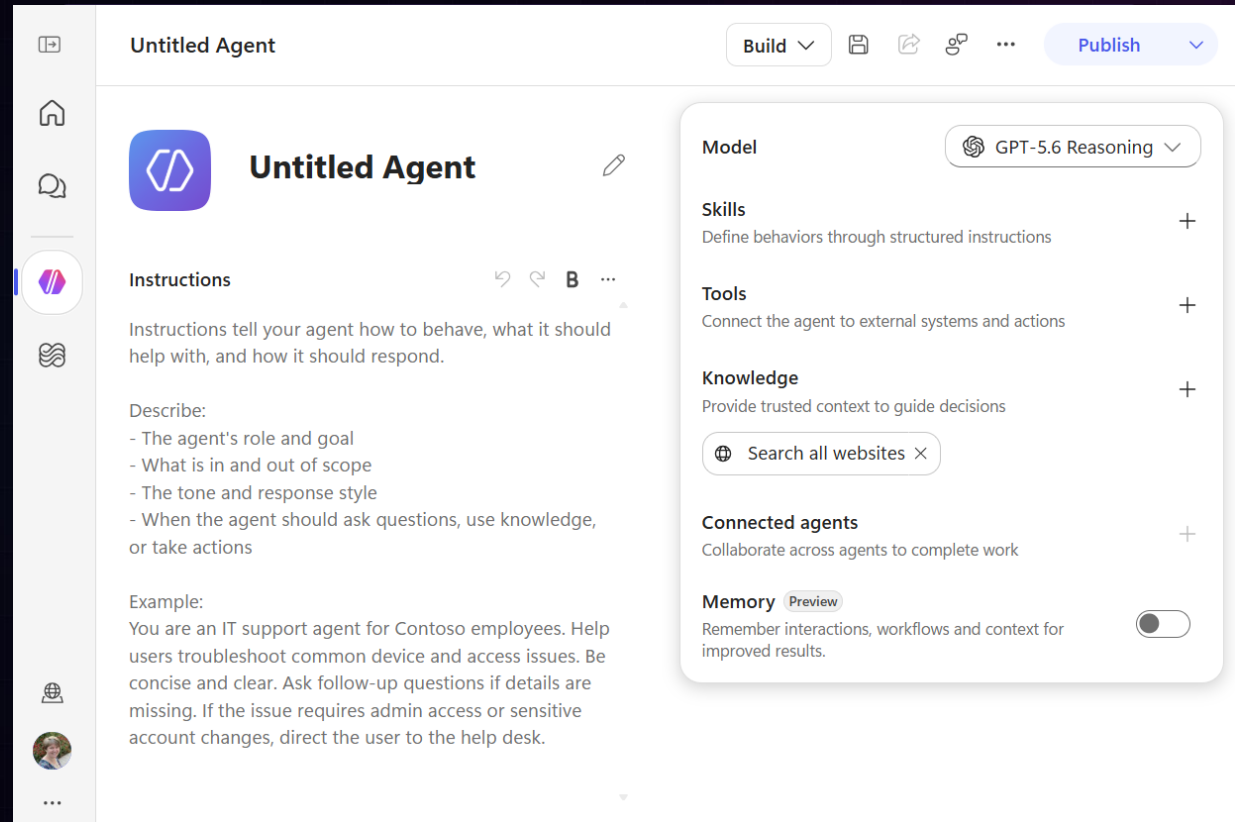


# Wer im Frühjahr Agenten gebaut hat, hat eine andere Plattform gelernt.

- Seit dem 17. Juni 2026 gibt es eine **neu gebaute Authoring-Experience** mit eigener Orchestrierungs-Runtime.
- Die bisherige Experience verschwindet nicht. Beide stehen nebeneinander, und du entscheidest dich pro Agent.
- Vieles, was in Blogposts vom Frühjahr steht, beschreibt ein Produkt, das so nicht mehr gebaut wird.

## MERKSATZ

***Ein Agent, der antwortet, ist eine bessere Suche.  
Interessant wird er erst, wenn er handelt.***



# Drei Brüche, die in jedes laufende Agenten-Projekt hineinregieren.

01

## Topics sind weg

In der neuen Experience gibt es keine Topics und keine Verzweigungslogik. Du beschreibst das Verhalten in natürlicher Sprache, der Orchestrator entscheidet über Wissen und Werkzeuge.

02

## Identität ist Pflicht

Seit Juli 2026 legt Copilot Studio für jeden neuen Agenten automatisch eine Entra Agent ID an. Ein Opt-out auf Environment-Ebene gibt es nicht mehr.

03

## Der Zähler startet früher

Auf der neuen Runtime kosten schon Bauen, Vorschau, Testen und Evaluieren Credits. Nicht erst der Betrieb.

*Keiner der drei Punkte ist ein Feature. Alle drei sind Annahmen, die in einem Projektplan stehen könnten.*



E I N S A T Z

# 02

## DAS PRINZIP

Nicht das Modell entscheidet, was dein Agent kann. Die Runtime entscheidet.



# Der Harness ist die Runtime zwischen deinem Design und dem Modell.

01

## GitHub Copilot harness

Für mehrstufige Prozesse. Nimmt ein Ziel, zerlegt es, ruft Werkzeuge, korrigiert sich bei Fehlern. Erzeugt Word, Excel, PowerPoint und PDF. Skills und Memory. Abrechnung über Credits.

02

## Standard harness

Für regelbasierte Agenten und strukturierte Abläufe. Du definierst Topics, Prompts und Pfade, das Ergebnis ist vorhersagbar. Lizenzmodell wie bisher.

03

## Copilot chat harness

Für die Erweiterung von Microsoft 365 Copilot Chat um eigenes Wissen. Nur intern veröffentlichbar. Verbrauch oder in der Copilot-Lizenz enthalten.

*Die Harness-Wahl bestimmt Fähigkeiten, Kanäle und Rechnung. Sie ist keine Einstellung, sondern eine Architekturentscheidung.*



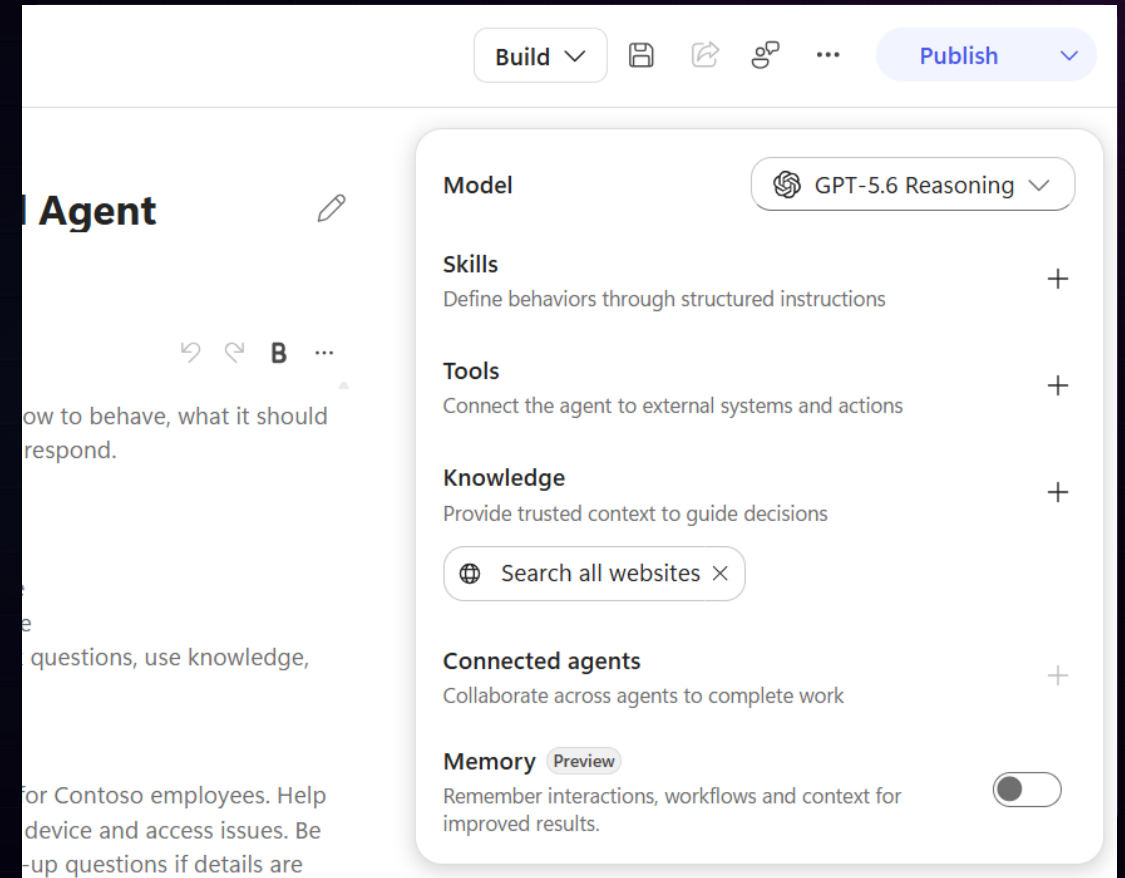


# Sechs Bauteile. Weniger reicht nicht, mehr braucht es nicht.

- **Instructions:** Rolle, Ton, Ziele, Grenzen. In natürlicher Sprache, kein Flussdiagramm.
- **Knowledge und Tools:** was der Agent als wahr annehmen darf, und was er tun darf.
- **Skills:** wiederverwendbare Instruktionsbausteine, einmal schreiben, in mehreren Agenten nutzen.
- **Memory und Connected Agents:** Kontext über Sitzungen hinweg, Delegation an Spezialisten.

## MERKSATZ

***Wer keine Grenzen schreibt, hat keine gesetzt.  
Instructions sind Governance, nicht Kosmetik.***

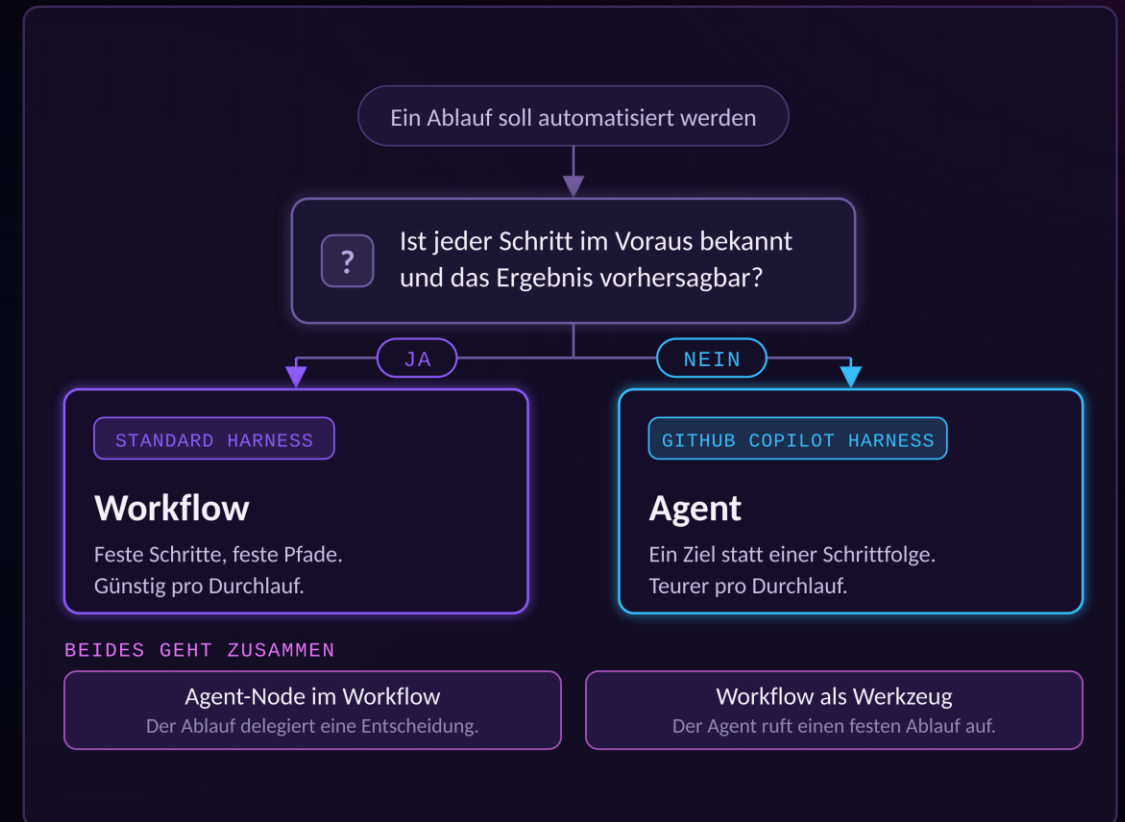


# Die erste Frage ist nie das Modell, sondern: braucht das überhaupt Reasoning?

- Ablauf immer gleich, Ergebnis vorhersagbar? Dann ist es ein **Workflow** und kein Agent.
- Variable Eingaben, Ausnahmen, Zwischenentscheidungen? Dann lohnt sich **Reasoning**.
- Beides kombiniert: ein Agent-Node im Workflow, oder ein Workflow als Werkzeug im Agenten.
- **Human-in-the-Loop** ist eingebaut. Ein Schritt pausiert, holt eine Freigabe, läuft weiter.

## MERKSATZ

***Der Agent ist das Gesicht. Die Arbeit macht der Workflow.***



E I N S A T Z

# 03

## DER BAUKASTEN

Power Platform: Abläufe finden, automatisieren und mit Kontext versorgen.



# Drei Schritte, in dieser Reihenfolge. Wer bei drei anfängt, baut Demos.

01

## Identifizieren

Wo entstehen Wartezeiten, Rückfragen und Copy-Paste? Process Mining und Analytics zeigen es. Nicht der lauteste Wunsch gewinnt, sondern der messbare Ablauf.

02

## Automatisieren

Erst den deterministischen Teil als Workflow bauen. Was danach noch wackelt, bekommt einen Agenten davor. Nicht umgekehrt.

03

## Anreichern

Wissen, Connectoren, MCP-Server, Microsoft IQ. Kontext ist der Unterschied zwischen einer Antwort und einer brauchbaren Antwort.

*Der Baukasten ist nicht das Problem. Die Auswahl ist es.*

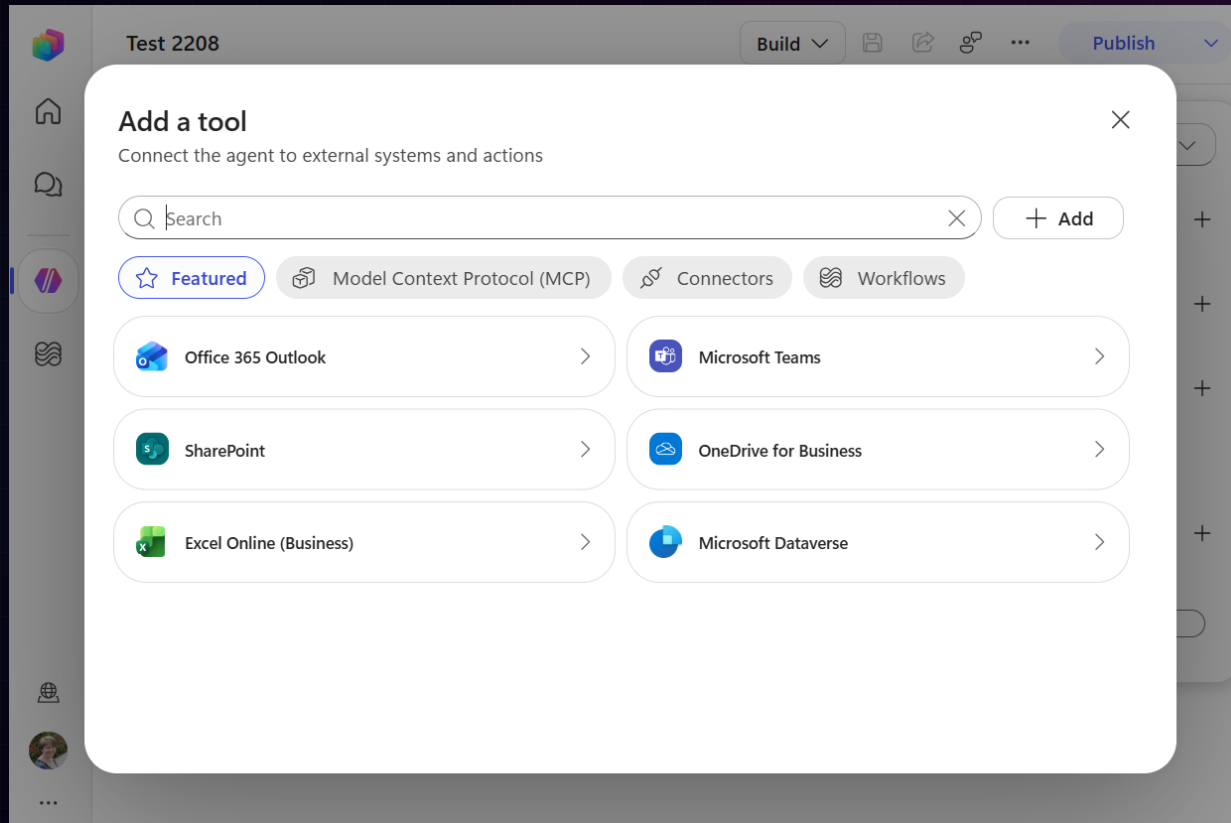


# Kontext kommt aus vier Richtungen. Jede hat einen anderen Preis.

- **Knowledge:** SharePoint mit Metadatenfiltern, Dateien, Websites, Dataverse, Azure AI Search.
- **Microsoft IQ:** E-Mails, Termine, Dateien, Teams-Nachrichten und Personendaten aus dem Tenant.
- **Tools:** Connectoren, REST-APIs und MCP-Server. Seit Juli lassen sich MCP-Server zertifizieren.
- **Foundry IQ:** eine in Microsoft Foundry aufgebaute und getunte Wissensbasis andocken.

## MERKSATZ

***Jede Kontextquelle kostet Credits und vergrößert die Angriffsfläche. Beides gehört in dieselbe Entscheidung.***



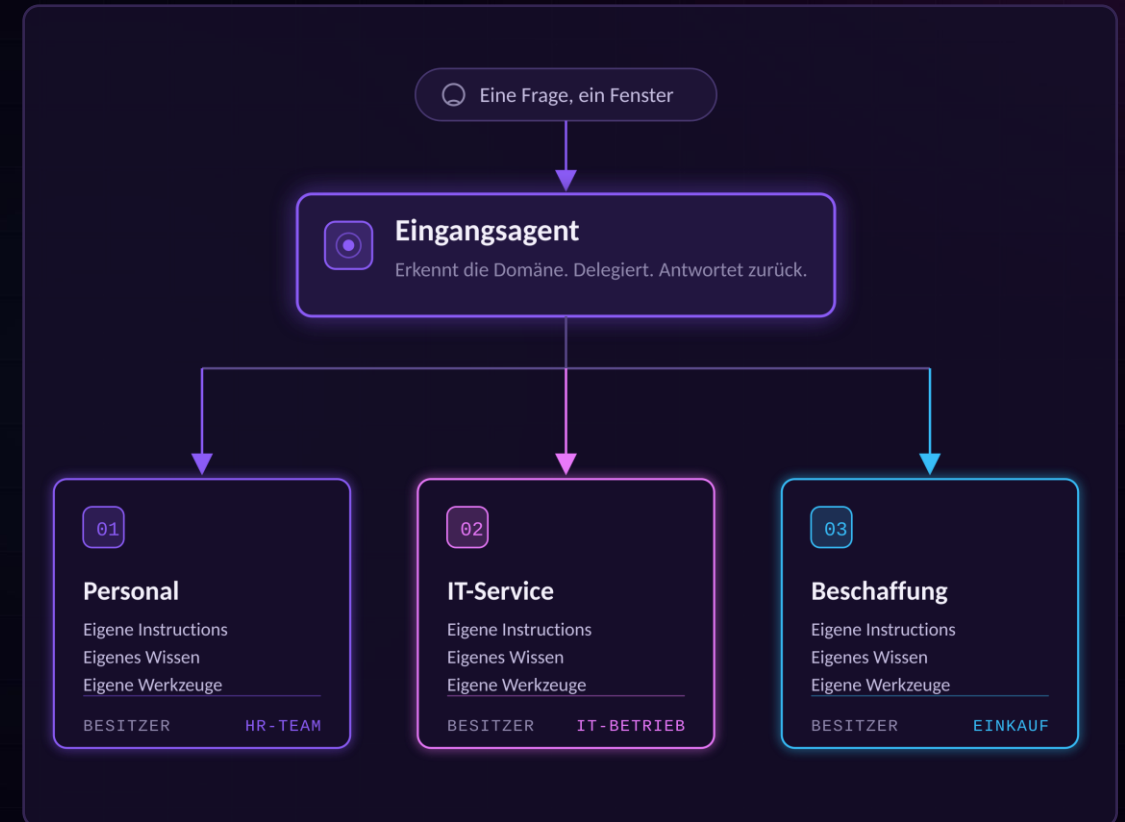


# Ein Agent für alles wird unwartbar. Deshalb: eine Eingangstür, dahinter Spezialisten.

- **Connected Agents:** der Hauptagent delegiert an Fachagenten mit eigenen Instructions und Werkzeugen.
- Jedes Team besitzt seinen eigenen Agenten. Neue Fähigkeit heißt neuer Agent, nicht längere Instructions.
- Grenze: in der neuen Experience lassen sich derzeit nur in Copilot Studio gebaute Agenten verbinden.
- Über das **A2A-Protokoll**, seit April 2026 GA, geht die Verbindung auch nach außen.

## MERKSATZ

***Wenn deine Instructions zwei Bildschirmseiten füllen, brauchst du keinen besseren Prompt, sondern einen zweiten Agenten.***



# Demo



## EINEN HANDELNDEN AGENTEN BAUEN



E I N S A T Z

# 04

## DIE VERTEILUNG

Zwischen dem fertigen Agenten und dem benutzten Agenten liegen drei Freigaben.



# Drei Wege nach draußen. Sie führen nicht zum selben Ziel.

01

## Teilen

Agent Builder, Share-Dialog: Can edit oder Can chat. Direkter Zugriff für benannte Personen. Kein Rollout, keine weiteren Kanäle.

02

## Org-Katalog

Aus Agent Builder zur Prüfung einreichen. Nach Freigabe im Admin Center erscheint der Agent unter Built by your org im Agent Store.

03

## Kanäle

Copilot Studio, Bereich Channels: Microsoft 365 Copilot, Teams, Web, Telefonie. Freigabe läuft über das Copilot Control System.

*Gebaut ist nicht verteilt. Wer das erst beim Rollout merkt, verliert zwei Wochen an eine Admin-Warteschlange.*

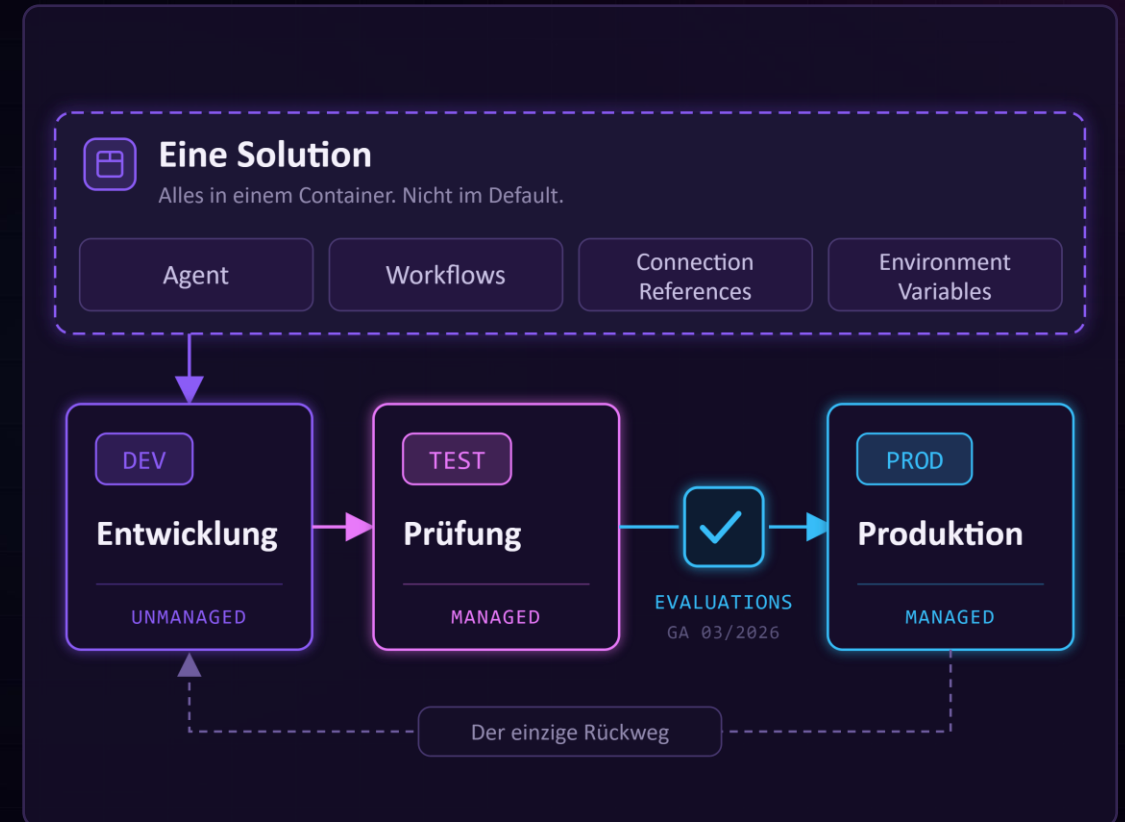


# Skalierbar heißt: der Agent überlebt einen Umgebungswechsel.

- Alles in eine **Solution**, von Anfang an. Was in der Default-Solution entsteht, lässt sich nicht sauber weiterreichen.
- **Connection References** statt fest verdrahteter Verbindungen, Environment Variables statt fester Werte.
- Power Platform **Pipelines** schieben von DEV über TEST nach PROD, im Ziel automatisch als managed.
- **Agent-Evaluations** mit Testsets als Qualitätstor vor dem Deployment.

## MERKSATZ

***Der häufigste Fehler ist nicht technisch. Er passiert in Minute eins, wenn niemand eine Solution anlegt.***



# Ein Agent ist ab jetzt ein Identitätsobjekt, kein Feature.

- Entra Agent ID: seit Juli 2026 automatisch für jeden neuen Agenten, ohne Opt-out auf Environment-Ebene.
- Damit greifen Conditional Access, DLP und Connector-Berechtigungen pro Agent statt pro Umgebung.
- Agent 365 ist seit dem 1. Mai 2026 GA: beobachten, steuern, absichern. Kein Werkzeug zum Bauen.
- Preis: 15 USD pro Nutzer und Monat, oder enthalten in Microsoft 365 E7.

## MERKSATZ

**Die Frage ist nicht, ob Agenten Identitäten bekommen. Die Frage ist, wer sie besitzt, wenn der Ersteller kündigt.**

**Alle Agents** Agent 365

Überwachen und verwalten Sie Agents in Ihrer Organisation, einschließlich Agents, die Aufmerksamkeit benötigen, Agents ohne B...

[zum Verwalten von Agents](#)

Registrierung Zuordnen **Frontier** Anforderungen Lokale Agents **Frontier**

Benutzerdefiniertes Tagging ist verfügbar. Organisieren Sie Ihre Agents mit Tags, damit sie leichter gefunden, gefiltert und...

Agents insgesamt 299 Gefährdete Agents — Agents ohne Besitzer 0

Verbundene P Erste Schritte

Status Herausgebertyp Plattform Kanal Es werden 50 von insgesamt 299 Agents angezeigt Suchen

| Name           | Status    | Plattform      | Risiken |
|----------------|-----------|----------------|---------|
| re:Members AMS | Verfügbar | re:Members AMS | 0       |
| Fluix          | Verfügbar | Fluix          | 0       |
| Avvoka MCP     | Verfügbar | Avvoka MCP     | 0       |



# Auf der neuen Runtime läuft der Zähler ab dem Bauen, nicht ab dem Betrieb.

- Credits decken drei Dinge ab: die Tokens des Modells, die Werkzeuge inklusive Wissen und MCP, und die Runtime selbst.
- Bauen, Vorschau, Testen und das Erzeugen von Evaluations verbrauchen Credits.
- Beahlt wird über den Meter mit 0,01 USD je Credit oder über Pakete zu 200 USD für 25.000 Credits im Monat.
- Nicht verbrauchte Credits eines Pakets verfallen zum Monatsende.

## MERKSATZ

**Rechne die Bauphase ein. Zehn Leute, die eine Woche experimentieren, sind eine eigene Position im Budget.**

## Cost Management

Überwachen Sie die Nutzung von KI-Guthaben, konfigurieren Sie die Abrechnung, legen Sie Ausgabenlimits fest und verwalten Sie Ihre Kosten. [Informationen zur Kostenverwaltung](#)

**i** Gilt für **Copilot Cowork** und **Work IQ API** im Moment. Während wir daran arbeiten, mehr Agents und Dienste für diese Erfahrung bereitzustellen, wird die nutzungsbasierter Bezahlung in [klassische Abrechnung & Verbrauch](#).

Übersicht Konfiguration **Verbrauch**

Zeigen Sie Benutzer, Gruppen, Agents und Dienste mit Guthabennutzung während des ausgewählten Datumsbereichs an.

### Nutzung von Copilot-Guthaben

|          |         |                    |
|----------|---------|--------------------|
| Benutzer | Gruppen | Agents und Dienste |
| 0        | 0       | 0                  |

Microsoft 365 Copilot-Lizenz

Agents and services

0 Elemente

Benutzer suchen...

Monat bis heute

Exportieren

Spalten verwalten

# Demo



## DIE INVENTUR: WER LÄUFT HIER EIGENTLICH?

Ich zeige keinen Agenten, sondern die Liste aller Agenten. Und wer sie freigegeben hat.



# Drei Dinge, die bleiben.

1

## Die Runtime ist die Entscheidung

Der Harness kommt vor dem Modell. Er legt fest, was der Agent kann, wo er landet und was er kostet.

2

## Gebaut ist nicht verteilt

Teilen, Org-Katalog und Kanäle sind drei verschiedene Wege mit drei verschiedenen Freigaben.

3

## Der Agent hat eine Identität

Seit Juli automatisch. Damit wird aus einem Bastelprojekt ein Objekt mit Besitzer, Rechten und Protokoll.

*Nächster Schritt: eine Woche lang zählen, wie viele Agenten in eurem Tenant laufen. Die Zahl überrascht fast jeden.*

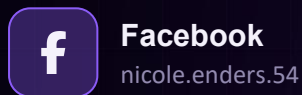
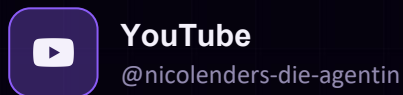
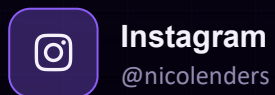
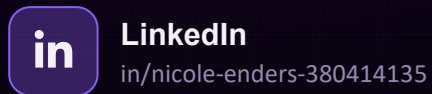




# DANKE.

Fragen, Widerspruch und Praxisberichte sind ausdrücklich erwünscht.

KONTAKT · KEINE LOSEN ENDEN



 nicole.enders.de@gmail.com



WEBSITE

**nicolenders.com**

Identitäten, Einsätze, Briefings und  
Depeschen an einem Ort.



FOLIEN ZUM VORTRAG

**nicolenders.com/briefings**

Alle Briefings mit Slides,  
Aufzeichnungen und Terminen.

*Die Folien stehen nach dem Vortrag online — Scannen genügt,  
kein Mitschreiben nötig.*