

Microsoft 365 Copilot: Neue Enterprise-Funktionen

Executive Summary

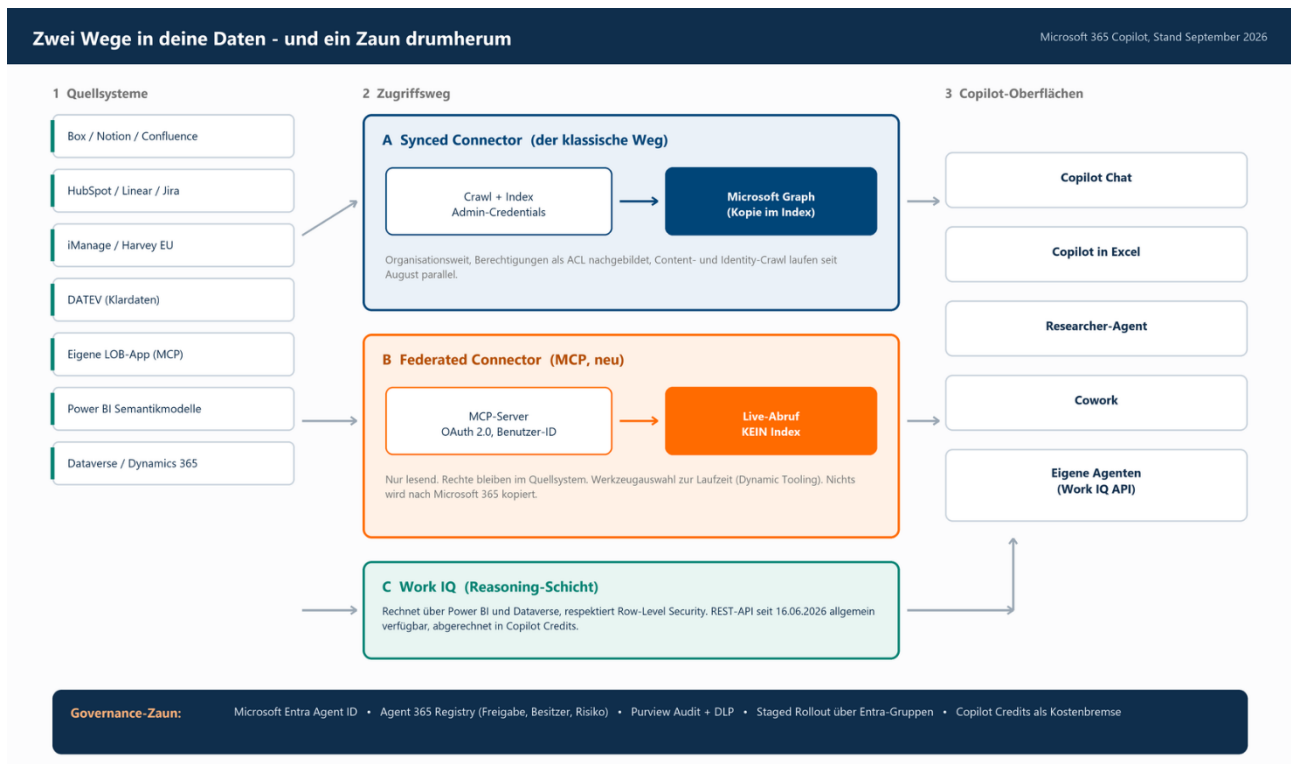
Copilot war zwei Jahre lang ein sehr teurer Textvorschlagsautomat mit Lizenzschlüssel. Das ist vorbei. Was Microsoft zwischen Juni und August 2026 ausgerollt hat, verändert nicht die Oberfläche, sondern den Unterbau: Copilot holt sich Daten jetzt live aus Fremdsystemen, ohne sie vorher zu indexieren. Er rechnet über Power BI und Dataverse. Und er hat eine eigene Verwaltungsebene für Agenten bekommen, samt Identität, Besitzer und Risikobewertung. Für dich heißt das: Die Diskussion verschiebt sich von „Wer bekommt eine Lizenz?“ zu „Wer darf welchen Agenten wie lange laufen lassen?“.

Drei Bausteine musst du kennen. Erstens die Federated Connectors auf Basis des Model Context Protocol: Sie ziehen Daten in Echtzeit aus Box, HubSpot, Notion, iManage, DATEV oder deiner eigenen Line-of-Business-Anwendung, mit der Identität des Anwenders, ohne eine einzige Kopie in Microsoft 365. Zweitens Work IQ, die Schicht, die Microsoft 365, Dynamics 365 und Power Platform zusammendenkt und seit dem 16. Juni 2026 eine eigene REST-API hat. Drittens Agent 365 als Registry und Kontrollebene im Microsoft 365 Admin Center, in der zum ersten Mal steht, wie viele Agenten in deinem Tenant eigentlich herumlaufen. Die Antwort auf diese Frage überrascht in fast jedem Projekt, und selten angenehm.

Die unangenehme Nachricht steht auf der Rechnung. Die teuerste Zeile deiner Copilot-Kosten ist ab sofort nicht mehr die Lizenz. Agentenlaufzeit wird in Copilot Credits gemessen und obendrauf abgerechnet. Wer 2024 stolz war, dass er zweihundert Copilot-Lizenzen sauber verteilt hat, hat 2026 eine Kostenposition, die niemand budgetiert hat und die im Zweifel nachts weiterläuft.

FAKTEN

Die Eckdaten in einer Zeile: Work IQ APIs seit 16.06.2026 allgemein verfügbar und in Copilot Credits abgerechnet. E7 Frontier Suite seit 01.07.2026 für 99 US-Dollar pro Nutzer und Monat, darin enthalten Microsoft 365 E5, Copilot, Agent 365 und die Entra Suite. Federated Connectors seit 15.07.2026 im Admin Center verwaltbar. Der einheitliche Work-IQ-Endpunkt für Agenten und Workflows löst seit 25.08.2026 die alten Copilot-Chat-Schnittstellen ab.



Grafik 1: Die zwei Zugriffswege auf Unternehmensdaten und die Governance-Schicht, die beide umschließt.

Worum geht es im Detail?

Federated Connectors: die Daten bleiben, wo sie sind

Der klassische Copilot-Connector war ein Staubsauger. Er hat mit Admin-Zugangsdaten ein Fremdsystem gecrawlt, den Inhalt in den Microsoft-Graph-Index geschaufelt und die Berechtigungen als ACL nachgebaut. Das funktioniert, kostet aber Speicher, Zeit und Nerven — und der Betriebsrat stellt zu Recht Fragen, warum eine Kopie sämtlicher Personalakten plötzlich in einem Suchindex liegt.

Federated Connectors drehen das Prinzip um. Sie sprechen über das Model Context Protocol mit dem Quellsystem und holen die Information erst dann, wenn jemand fragt. Nichts wird indexiert, nichts kopiert, nichts gespeichert. Die Authentifizierung läuft per OAuth 2.0 mit der Identität des Anwenders, nicht mit einem Dienstkonto. Wer im Quellsystem nichts sehen darf, sieht auch in Copilot nichts. Der Zugriff ist ausschließlich lesend und in Microsoft Purview auditierbar. Unterstützt werden derzeit Copilot Chat, Copilot in Excel, der Researcher-Agent und Cowork.

Der Katalog ist inzwischen erstaunlich breit und in Kategorien sortiert: Box und Notion bei den Dokumenten, HubSpot, Intercom und Clarify im CRM, Linear, Quire und Azure DevOps in der IT, iManage, Everlaw und Harvey im juristischen Umfeld — Harvey sogar mit eigener EU-Variante. Für den deutschsprachigen Mittelstand besonders interessant: der DATEV-Connector von Klarden. Dazu kommen Finanzdatenquellen wie Moody's, S&P Global, FactSet und Morningstar sowie ein ganzer Block aus Medizin und Forschung von PubMed bis ClinicalTrials.gov.

Die Verwaltung sitzt im Microsoft 365 Admin Center unter Copilot connectors und dort im Reiter „Your connections“. Synchronisierte Konnektoren, föderierte Konnektoren und die unterstützten Cowork-Plugins liegen zum ersten Mal an einer Stelle. Du kannst je Konnektor tenantweit an- und

ausschalten und über „Add staging“ einen gestaffelten Rollout auf bestimmte Entra-ID-Gruppen begrenzen. Genau das ist die Funktion, mit der du eine Pilotgruppe aufbaust, statt einen Big Bang zu veranstalten und danach Feuerwehr zu spielen.

Kriterium	Synced Connector	Federated Connector (MCP)
Datenhaltung	Kopie im Microsoft-Graph-Index	Keine Kopie, Live-Abruf zur Laufzeit
Anmeldung	Admin-Credentials, organisationsweit	Anmeldedaten des Anwenders, je Benutzer
Berechtigungen	Als ACL nachgebildet, Crawl-abhängig	Vom Quellsystem durchgesetzt, immer aktuell
Aktualität	So frisch wie der letzte Crawl	Sekundenaktuell
Schreibzugriff	Nein	Nein, ausschließlich lesend
Typischer Einsatz	Große, stabile Wissensbestände	Bewegte Daten: Tickets, Deals, Kurse, Akten
Neue Abhängigkeit	Crawl-Fenster und Indexgröße	Verfügbarkeit und Latenz des MCP-Servers

WARNUNG

Von Microsoft veröffentlichte Federated Connectors sind standardmäßig für deinen Tenant aktiv. Du deaktivierst, du aktivierst nicht. Der Sammelschalter heißt jetzt „Allowed agent types“ in den Agent-365-Einstellungen und ersetzt den früheren tenantweiten PowerShell-Schalter. Wer damals das Cmdlet benutzt hat, bekommt einen Message-Center-Beitrag mit der Aufforderung, die Entscheidung im Portal erneut zu treffen — und nach Ablauf der Frist gilt der alte Zustand schlicht nicht mehr. Das ist kein Bug, das ist eine Deadline mit Ansage.

Work IQ: die Schicht, die alles zusammenrechnet

Work IQ ist der Teil, den man in Demos kaum sieht und im Betrieb am meisten merkt. Es ist die Ebene, die Signale aus Microsoft 365, Dynamics 365 und der Power Platform zusammenführt. Konkret: Copilot beantwortet Fragen jetzt aus Power-BI-Berichten und Semantikmodellen heraus und respektiert dabei die Row-Level Security. Das klingt nach einer Fußnote und ist in Wahrheit das Ende einer ganzen Gattung von Bastellösungen: Niemand muss mehr CSV-Dateien aus Power BI exportieren, damit die Vertriebsauswertung im Chat landet. Dazu kommt die Suche und Abfrage über Dataverse, womit die klassischen Line-of-Business-Datensätze im Chat auftauchen.

Für Entwickler ist die eigentliche Nachricht die Work IQ API, die am 16. Juni 2026 allgemein verfügbar wurde. Sie besteht im Kern aus drei Teilen: Die Chat API liefert die Antwort, die Copilot einem Anwender geben würde, inklusive Zitaten. Die Context API liefert bewusst keine fertige Antwort, sondern den aufbereiteten Kontext in einem Format, das ein eigener Agent weiterverarbeiten kann. Und die Tools bieten Verben für Microsoft-365-Aktionen wie Mail senden, Termin planen oder Dokument hochladen. Ergänzt wird das durch Unterstützung für das Agent-to-Agent-Protokoll und einen neu gebauten Remote-MCP-Server. Seit dem 25. August 2026 gibt es obendrein einen einheitlichen REST-Endpunkt für Agenten und Workflows, der die verstreuten

alten Copilot-Chat-Endpunkte ersetzt. Wenn dein Haus in den letzten anderthalb Jahren etwas gegen diese Endpunkte gebaut hat, steht jetzt Migrationsarbeit an.

WICHTIG

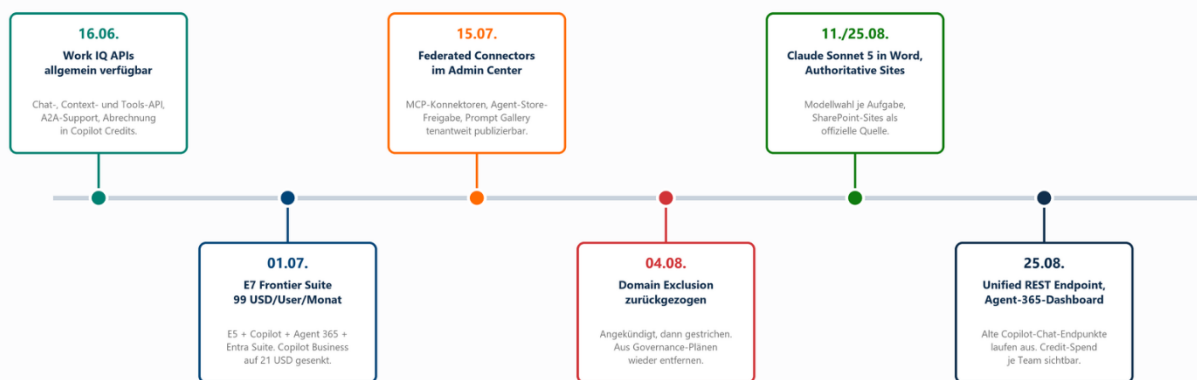
Die Work IQ API hat kein eigenes SKU und keine Lizenz pro Nutzer. Sie wird verbrauchsabhängig in Copilot Credits abgerechnet. Das ist bequem für den Einkauf und gefährlich für die Fachabteilung: Ein schlecht gebauter Agent, der im Minutentakt Kontext abrufen, verursacht keine Fehlermeldung, sondern eine Rechnung.

Agent 365: das Melderegister für deine Agenten

Der Agent-Bereich im Microsoft 365 Admin Center ist die Kontrollebene, die dem Wildwuchs der letzten zwei Jahre hinterhergebaut wurde. Die Registry erfasst Agenten aus Copilot Studio, dem Agent Builder, SharePoint, Foundry und dem Agents Toolkit — und über den Registry-Sync sogar Agenten von Nicht-Microsoft-Plattformen wie Manus oder Genspark. Die Kennzahlen im Überblick sind bewusst unbarmherzig gewählt: Gesamtzahl der Agenten, aktive Nutzer der letzten dreißig Tage und Agentenlaufzeit in Stunden.

Interessanter als die Zahlen sind die Handlungskarten. „Agents without owners“ zeigt dir Agenten ohne Besitzer, also die digitalen Fundstücke, die weiterlaufen, obwohl der Erbauer längst das Unternehmen verlassen hat. „Agents at risk“ bündelt hochschwere Risikosignale aus Entra, Defender und Purview an einer Stelle. Dazu kommen offene Freigabeanfragen und Agenten mit Fehlern. Wichtig für dein Rollenkonzept: Freigeben und Besitzer zuweisen darf nur der AI Administrator oder der Global Administrator. Die Rolle AI Reader sieht alles und darf nichts — genau richtig für Revision, Datenschutz und den Kollegen aus dem Controlling, der eigentlich nur wissen will, wer das Geld verbrennt.

Was tatsächlich ausgerollt wurde - Juni bis September 2026



Lesehilfe: Alles oberhalb der Achse betrifft Plattform und Datenzugriff, alles unterhalb Lizenz, Geld und Verwaltung.

Grafik 2: Die Rollout-Chronologie. Oberhalb der Achse Plattform und Datenzugriff, unterhalb Lizenz, Geld und Verwaltung.

Der Kleinkram, der in Summe mehr bringt

Neben den drei großen Bausteinen ist eine Menge Handwerk gelandet, das im Alltag mehr Wirkung entfaltet als jede Keynote-Folie. SharePoint kennt jetzt Authoritative Sites: Du erklärst bestimmte Sites zur offiziellen Quelle, und Copilot gewichtet deren Inhalte in der Suche höher. Das

ist die Antwort auf das klassische Problem, dass Copilot die Reisekostenrichtlinie von 2019 aus dem Archiv einer aufgelösten Abteilung zitiert. Agenten aus dem Agent Builder können nach Admin-Prüfung in den Bereich „Built by your org“ des Agent Store eingereicht werden, und die Prompt Gallery lässt sich tenantweit mit kuratierten Sammlungen bestücken.

Bei den Konnektoren gibt es verschachtelte Berechtigungen für Confluence und ServiceNow, sodass Rechte auf Elternebene bei untergeordneten Elementen ausgewertet werden. Content- und Identity-Crawl laufen parallel, was die Zeit bis zur Verfügbarkeit neuer Inhalte spürbar drückt. Private Inhalte aus Viva Engage dienen als Grounding-Quelle, natürlich nur im Rahmen der vorhandenen Berechtigungen. Auf der Verwaltungsseite kamen im August ein deutlich erweitertes Cost-Management-Dashboard, eine Ansicht des Credit-Verbrauchs je Team, eine Heatmap darüber, welche Sites deine Agenten anfassen, sowie Purview-Kontrollen für Cowork hinzu. In der Vorschau steckt eine DLP-Regel, die externe E-Mails aus dem Grounding heraushält — der schlichteste und wirksamste Schutz gegen Prompt Injection per Posteingang, den Microsoft bisher gebaut hat.

Bei den Modellen ist Wahlfreiheit eingezogen. In Word kannst du seit dem 11. August zwischen Anthropic- und OpenAI-Modellen wählen, Claude Sonnet 5 ist für anspruchsvollere Aufgaben als Standard gesetzt. Der Researcher-Agent lässt die Modellwahl direkt im Chat zu. In Cowork gibt es Claude Fable 5 als abgeschaltete Vorschau für lange, mehrstufige Arbeiten.

WARNUNG

Bei der Fable-5-Vorschau in Cowork werden Prompts und Antworten beim Modellanbieter aufbewahrt. Das ist sauber dokumentiert und trotzdem der Punkt, an dem dein Datenschutzbeauftragter das Gespräch beenden wird, wenn du es ihm erst nach dem Rollout erzählst. Vorschau bleibt standardmäßig aus, bis das Verzeichniss steht.

Was sind Chancen? Was sind Risiken?

Die größte Chance ist unspektakulär: Du sparst dir eine ganze Bauphase. Wer bisher Fachdaten in Copilot bringen wollte, hat ein Integrationsprojekt aufgesetzt, Indexstrategien diskutiert, Berechtigungen nachgebaut und am Ende ein Konstrukt betrieben, das bei jedem Schema-Wechsel im Quellsystem gewackelt hat. Mit föderierten Konnektoren fällt dieser Bauteil weg. Die Ersparnis ist nicht nur Geld, sondern Risiko, das du nicht mehr trägst.

Der zweite große Vorteil ist juristischer Natur. Keine Kopie bedeutet keine zusätzliche Verarbeitungsstelle, keinen zweiten Löschprozess und kein Erklären, warum ein gelöschter Datensatz im Index noch zwei Wochen weiterlebt. Wenn du dich schon einmal in einem Meeting mit Rechtsabteilung, Betriebsrat und Datenschutzbeauftragtem wiedergefunden hast, weißt du, was dieses Argument wert ist. Und drittens ersparen dir die Work IQ APIs, die Graph-Klempnerei selbst zu schreiben — Kontext und Werkzeuge kommen fertig, du baust nur noch die Fachlogik.

Die Risiken sind nicht theoretisch, sondern zählbar. Sie stehen in der folgenden Tabelle, jeweils mit der Gegenmaßnahme, die tatsächlich funktioniert.

Risiko	Was konkret passiert	Was du dagegen tust
--------	----------------------	---------------------

Konnektoren von allein aktiv	Microsoft-eigene föderierte Konnektoren sind standardmäßig an, auch künftig veröffentlichte.	„Allowed agent types“ deselektieren, dann einzeln freigeben und mit Staged Rollout auf Pilotgruppen begrenzen.
Alter PowerShell-Schalter verfällt	Der frühere tenantweite Schalter wird nach einer Frist nicht mehr berücksichtigt.	Message Center aktiv auswerten und die Entscheidung im Portal erneut setzen. Termin dafür in den Betriebskalender.
Credit-Verbrauch außer Kontrolle	Agentenlaufzeit wird in Stunden gemessen und in Credits abgerechnet, oben auf die Lizenz.	Budget je Team, Warnschwellen anlegen und im August geänderte Kostenwarnungen neu aufsetzen.
Herrenlose Agenten	Agenten laufen weiter, obwohl der Ersteller das Unternehmen verlassen hat.	Karte „Agents without owners“ wöchentlich abarbeiten, Besitzerpflicht in die Freigaberegeln schreiben.
Prompt Injection per Mail	Eine externe Mail enthält Anweisungen, die der Agent brav ausführt.	Purview-DLP-Kontrolle für externe Mails im Grounding einschalten, sobald sie den Vorschaustatus verlässt.
Neue Betriebsabhängigkeit	Fällt der MCP-Server des Anbieters aus, gibt es keine Antwort — es existiert kein Index als Netz.	Verfügbarkeit vertraglich regeln, Monitoring aufsetzen und kritische Wissensbestände weiterhin synchronisiert halten.
Angekündigtes verschwindet	Die Domain Exclusion wurde angekündigt und am 04.08.2026 wieder zurückgezogen.	Roadmap-Einträge nie als Zusage in Konzepte schreiben. Erst GA, dann Betriebshandbuch.

TIPP

Der ehrlichste Wert im ganzen Admin Center ist die Agentenlaufzeit in Stunden. Nimm sie in dein monatliches Reporting auf und stelle sie neben die Zahl der aktiven Nutzer. Wenn die Laufzeit steigt und die Nutzerzahl nicht, hast du keinen Erfolg, sondern eine Schleife.

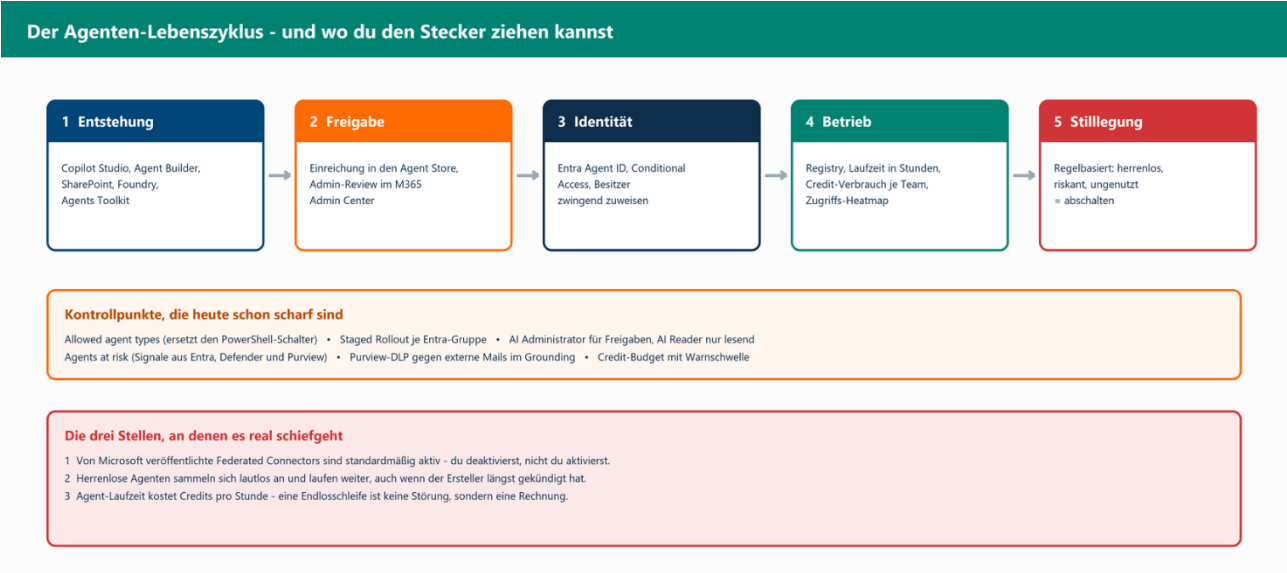
Was müssen wir jetzt schon vorbereiten?

Es gibt eine angenehme Nachricht: Fast alles, was jetzt zu tun ist, ist Verwaltungsarbeit und kein Entwicklungsprojekt. Es gibt auch eine unangenehme: Verwaltungsarbeit bleibt in Organisationen gern liegen, bis sie teuer wird. Fang bei der Bestandsaufnahme an. Öffne den Agent-Bereich im Admin Center und sieh dir die Registry an, bevor du irgendetwas planst. Die Zahl der Agenten und ihrer Erstellungsplattformen ist in aller Regel die beste Grundlage für ein Gespräch mit der Geschäftsführung, weil sie ohne Folienzauber auskommt.

Danach kommt die Freigabelogik. Entscheide bewusst, ob Microsoft-eigene und Partner-Konnektoren standardmäßig verfügbar sein sollen, und dokumentiere die Entscheidung. Partnerkonnektoren musst du ohnehin einzeln genehmigen. Setze anschließend das Rollenmodell auf: AI Administrator für Freigaben, AI Reader für Revision und Controlling. Wer heute noch Global Administrator verteilt, damit jemand eine Kennzahl sehen kann, hat ein anderes Problem als Copilot.

Der dritte Block ist Geld. Lege Credit-Budgets je Team an, definiere Warnschwellen und prüfe die bestehenden Kostenwarnungen: Nach der Umstellung im August müssen Warnungen auf

bestehenden Richtlinien neu erstellt werden. Wer das überliest, hat ein Alarmsystem, das nur noch dekorativ ist. Vierter Block: Inhalte. Kennzeichne die verbindlichen SharePoint-Sites als Authoritative Sites, sonst zitiert Copilot weiter das Archiv. Und fünfter Block: Entwicklung. Prüfe, welche Eigenbauten gegen die alten Copilot-Chat-Endpunkte laufen, und plane die Migration auf den einheitlichen Work-IQ-Endpunkt ein, bevor sie zum Vorfall wird.



Grafik 3: Agenten-Lebenszyklus, aktive Kontrollpunkte und die drei typischen Bruchstellen im Betrieb.

Was	Wer	Bis wann	Aufwand
Agenten-Registry auswerten, Bestand dokumentieren	IT-Betrieb	innerhalb von 2 Wochen	1 Tag
„Allowed agent types“ bewusst setzen, Entscheidung dokumentieren	AI Administrator	innerhalb von 2 Wochen	0,5 Tage
Message-Center-Beitrag zum PowerShell-Schalter abarbeiten	IT-Betrieb	sofort	0,5 Tage
Rollen AI Administrator und AI Reader vergeben	Identity-Team	innerhalb von 4 Wochen	0,5 Tage
Credit-Budgets und Warnungen je Team neu aufsetzen	IT-Controlling	innerhalb von 4 Wochen	1 Tag
Agenten ohne Besitzer klären oder abschalten	Fachbereiche	innerhalb von 6 Wochen	laufend
Authoritative Sites festlegen	Information Management	innerhalb von 8 Wochen	2 Tage
Pilotgruppe für zwei föderierte Konnektoren aufsetzen	IT-Betrieb und Fachbereich	innerhalb von 8 Wochen	3 Tage
Eigenentwicklungen auf Work-IQ-Endpunkt migrieren	Entwicklung	innerhalb von 12 Wochen	projektabhängig

Ein Praxisbeispiel zum Schluss, weil es besser haftet als jede Empfehlung. Bei einem mittelständischen Maschinenbauer haben wir im Juli die Registry zum ersten Mal geöffnet. Erwartet wurden etwa fünfzehn Agenten, gefunden wurden über achtzig. Der meistgenutzte war

kein offizielles Projekt, sondern ein SharePoint-Agent, den eine Kollegin aus dem Vertriebsinnendienst gebaut hatte, um Angebotsvorlagen zu finden. Er war besser als alles, was die IT bis dahin geliefert hatte. Der zweitplatzierte Agent hatte keinen Besitzer mehr, lief seit vier Monaten unbeaufsichtigt und griff auf eine Site mit Gehaltsbändern zu. Beide Erkenntnisse kamen aus derselben Tabelle, an einem Dienstagvormittag. Die eine hat ein Projekt ausgelöst, die andere eine Meldung. Deshalb fängst du mit der Bestandsaufnahme an und nicht mit dem Konzept.

Häufig gestellte Fragen

Werden bei Federated Connectors Daten nach Microsoft 365 kopiert?

Nein. Föderierte Konnektoren rufen Inhalte über das Model Context Protocol zur Laufzeit direkt aus dem Quellsystem ab und indexieren nichts in Microsoft 365. Die Anmeldung erfolgt per OAuth 2.0 mit der Identität des jeweiligen Anwenders, die Berechtigungen setzt weiterhin das Quellsystem durch, und der Zugriff ist ausschließlich lesend.

Brauche ich für Agent 365 die neue E7-Lizenz?

Nicht zwingend. Agent 365 lässt sich separat lizenzieren und ist zusätzlich in Microsoft 365 E7 enthalten, das seit dem 1. Juli 2026 für 99 US-Dollar pro Nutzer und Monat angeboten wird und E5, Copilot, Agent 365 und die Entra Suite bündelt. Ob sich das Bündel lohnt, hängt davon ab, wie viele dieser Bausteine du ohnehin einzeln kaufen würdest.

Was kostet ein Agent im laufenden Betrieb?

Die Sitzplatzlizenz deckt den Agentenbetrieb nicht vollständig ab: Agentenlaufzeit und API-Nutzung werden verbrauchsabhängig in Copilot Credits abgerechnet. Plane deshalb von Anfang an Budgets und Warnschwellen je Team ein und beobachte die Kennzahl Agentenlaufzeit in Stunden im Admin Center, weil sie schneller wächst als die Nutzerzahl.

Kann ich verhindern, dass neue Konnektoren automatisch verfügbar sind?

Ja. In den Agent-365-Einstellungen deaktivierst du unter „Allowed agent types“ die Optionen für von Microsoft und von Dritten veröffentlichte Konnektoren. Danach ist auch jeder künftig veröffentlichte Konnektor gesperrt, bis du ihn einzeln freigibst — dieser Schalter hat den früheren tenantweiten PowerShell-Befehl abgelöst.

Müssen bestehende Copilot-Integrationen angepasst werden?

Wahrscheinlich ja. Seit dem 25. August 2026 gibt es einen einheitlichen Work-IQ-REST-Endpunkt für Agenten und Workflows, der die verstreuten älteren Copilot-Chat-Schnittstellen ablöst. Prüfe deine Eigenentwicklungen auf betroffene Aufrufe und plane die Umstellung ein, bevor die alten Endpunkte abgeschaltet werden.