

CONSULTING BRIEFING SPEZIAL · KÜNSTLICHE INTELLIGENZ

Claude Duet: Wenn der KI-Assistent von selbst anklopft

Anthropics proaktiver Agent ist da – vorerst nur in den USA. Warum deine IT trotzdem schon jetzt eine Antwort braucht.

Executive Summary

Am 21. Oktober 2026 hat Anthropic **Claude Duet** als Research Preview vorgestellt. Duet ist kein weiterer Chat, sondern ein proaktiver Agent: Er schickt dir morgens einen Überblick, schaut alle paar Stunden in deine verbundenen Dienste und meldet sich, wenn eine Entscheidung ansteht. Aufgaben erledigt er auf einer eigenen virtuellen Maschine – auch dann, wenn dein Notebook längst zugeklappt ist.

Für deutsche Unternehmen ist Duet heute offiziell noch kein Thema: Zugang gibt es nur per Warteliste, nur für die Privat- und Power-User-Pläne Pro und Max und nur in den USA. Team- und Enterprise-Kunden sind außen vor. Genau darin liegt die Brisanz. Ein Agent, der ausdrücklich für Profis und Kleinunternehmer mit zu viel auf dem Zettel gebaut ist, landet erfahrungsgemäß zuerst über private Abos im Firmenalltag – lange bevor die IT eine Freigabe erteilt hat.

Die Empfehlung dieses Briefings: Nutze die Vorlaufzeit. Eine Richtlinie für proaktive Agenten, eine Positivliste für Konnektoren und ein früher Termin mit Datenschutzbeauftragtem und Betriebsrat kosten heute wenig – und sparen dir später die Feuerwehrübung.

FAKTEN | Claude Duet auf einen Blick (Stand: Oktober 2026)

- **Vorgestellt:** 21. Oktober 2026 als Research Preview, Zugang über eine Warteliste
- **Verfügbarkeit:** Pläne Pro und Max, nur USA; Team und Enterprise vorerst nicht
- **Modell:** Claude Opus 5.5
- **Plattformen:** eigene App für iOS und Android sowie im Browser auf claude.ai
- **Übernimmt aus dem Claude-Konto:** Memory, Skills und verbundene Apps (über 6.000 Konnektoren)
- **Arbeitsweise:** Morgen-Brief, Prüfung der Konten alle paar Stunden, Arbeit auf eigener VM mit Browser
- **Leitplanken:** Freigabe vor Senden, Bezahlen, Unterschreiben, Löschen; kein direkter Passwortzugriff; Classifier gegen das Weitergeben sensibler Daten
- **Kosten:** kein eigener Preis; Duet zehrt am bestehenden Nutzungskontingent

Worum geht es im Detail?

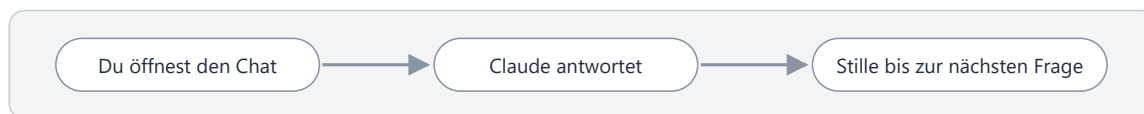
Vom Chatfenster zum Kollegen mit Schlüsselbund

Bisher lief die Arbeit mit Claude nach einem einfachen Muster: Du fragst, Claude antwortet, danach herrscht Funkstille. Selbst mit den Agentenfähigkeiten, die Anthropic im September in den normalen Chat integriert hat, bleibt der Mensch der Taktgeber. Duet dreht das um. Der Agent wartet nicht auf dich, sondern sortiert selbständig, was wichtig ist – und klopft nur an, wenn er dich wirklich braucht.

Man kann sich Duet wie einen digitalen Stabschef vorstellen: Morgens liegt ein Brief mit den wichtigsten Mails, Terminen und Vorgängen bereit. Tagsüber schaut er regelmäßig in Postfach, Kalender, Chat und Fachanwendungen. Gibst du ihm grünes Licht für eine Aufgabe, arbeitet er im Hintergrund weiter – vom

einfachen Terminabgleich bis zum Finanz-Dashboard. Intern lief das Projekt übrigens unter dem Namen „Claude Loop“, was die Idee ziemlich gut trifft.

Bisher: Chat (reaktiv)



Neu: Claude Duet (proaktiv)

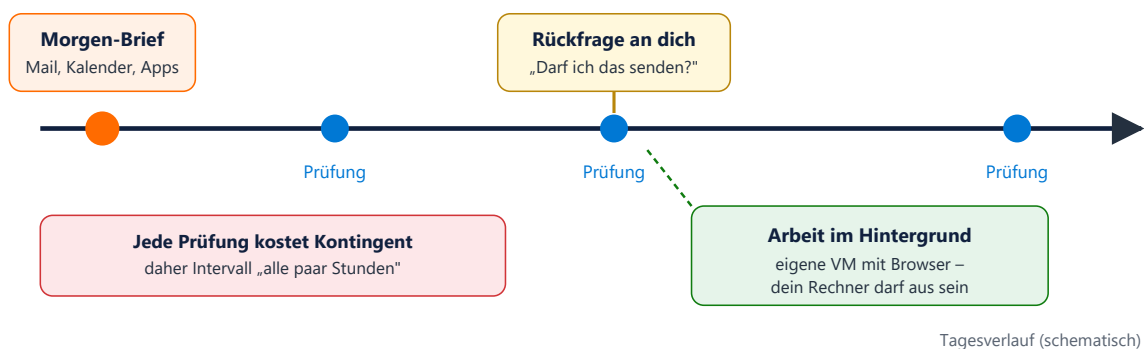


Abbildung 1: Reaktiver Chat gegenüber proaktivem Agenten im Tagesverlauf

Dass Duet nur „alle paar Stunden“ prüft und nicht im Minutentakt, ist kein Designfehler, sondern Ökonomie: Jede Prüfung ist ein Modellaufruf, und der geht vom Kontingent deines Plans ab. Anthropic sagt das selbst sehr offen – und schiebt nach, dass auch große Aufträge wie ein Finanzmodell oder eine Präsentation spürbar mehr Kontingent verbrauchen als ein normaler Chat.

Was unter der Haube steckt

Technisch setzt Duet auf Claude Opus 5.5 und übernimmt alles, was im Claude-Konto schon eingerichtet ist: Memory, Skills und verbundene Apps. Das ist bequem, denn die Einrichtung dauert praktisch null Minuten. Es ist aus Sicht der Unternehmens-IT aber auch der eigentliche Knackpunkt: Wer seinem privaten Claude-Konto irgendwann einmal das Firmenpostfach angeflanscht hat, schenkt diesen Zugriff Duet automatisch mit.

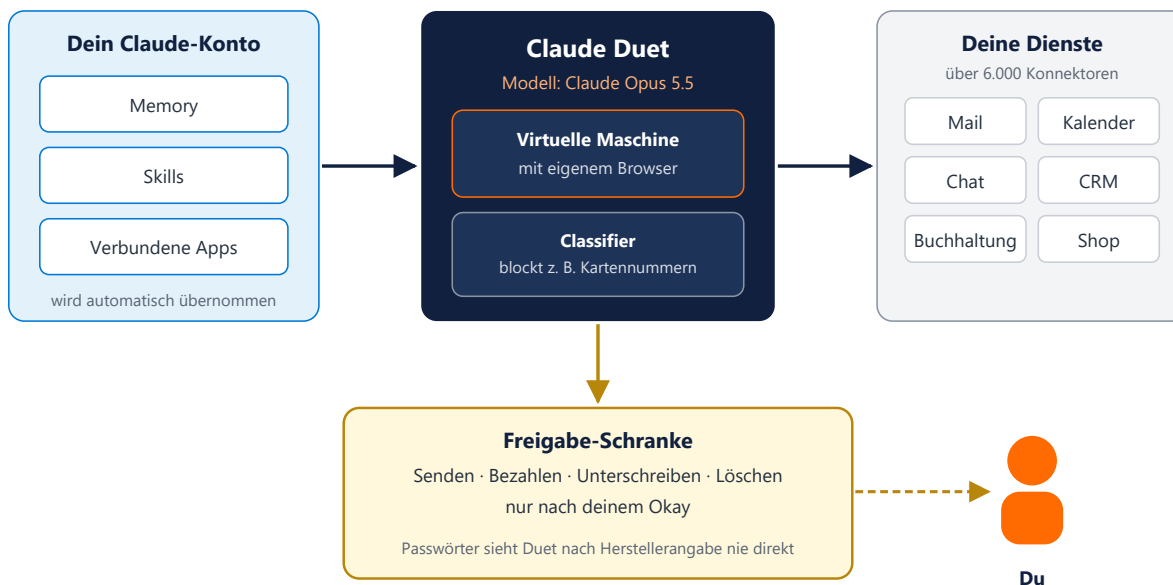


Abbildung 2: Bausteine von Claude Duet und die Freigabe-Schranke

Baustein	Was er tut	Was das für dich heißt
Morgen-Brief	Fasst die wichtigsten Punkte aus verbundenen Apps zusammen	Duet liest dafür regelmäßig Inhalte aus Mail, Kalender und Fachsystemen
Hintergrundprüfung	Schaut alle paar Stunden in die verbundenen Konten	Kontinuierlicher Datenzugriff statt punktueller Abfrage
Virtuelle Maschine	Erledigt Aufgaben mit eigenem Browser in der Cloud	Arbeit findet außerhalb deiner Endgeräte und deiner Netzwerkkontrolle statt
Konnektoren	Über 6.000 Anbindungen, z. B. Mail, Chat, CRM, Buchhaltung, Shop	Jeder Konnektor ist ein potenzieller Datenkanal nach außen
Freigabe-Schranke	Fragt vor Senden, Bezahlen, Unterschreiben, Löschen	Gutes Muster – aber nur so stark wie der Mensch, der „Ja“ tippt
Classifier	Verhindert das Weitergeben z. B. von Kartennummern	Schutz gegen grobe Fehler, kein Ersatz für Datenklassifizierung

Tabelle 1: Die Bausteine von Claude Duet aus Unternehmenssicht

Einordnung: Duet im Agenten-Zirkus

Anthropic ist mit Duet eher Nachzügler. Meta hat mit Muse einen Agenten für den privaten Alltag gestartet, OpenAI mit Dots einen Agenten für Projekte und Recherchen, die sich über Tage ziehen, und auch Grok Bot spielt in dieser Liga. Alle geben ihrem Agenten einen eigenen Rechner in der Cloud. Duet positioniert sich bewusst beim Arbeitsalltag von Berufstätigen und kleinen Unternehmen – also genau dort, wo Mails, Angebote und Rechnungen zu Hause sind.

Auch innerhalb der Anthropic-Familie lohnt eine saubere Abgrenzung, denn die Produktnamen purzeln gerade nur so heraus:

Angebot	Wofür es gedacht ist	Wer den Takt angibt
Claude (Chat und App)	Fragen, Analysen, Dokumente; übernimmt seit September auch längere Aufgaben	Du – Claude reagiert auf deine Anfrage
Claude Code	Softwareentwicklung im Terminal, in der IDE und im Web	Entwickler mit konkretem Auftrag
Claude Tag	Proaktiver Agent für Teams in Kollaborationstools, aktuell Slack	Das Team gemeinsam
Claude Duet	Persönlicher proaktiver Agent für den Arbeitsalltag	Duet selbst – du gibst frei

Tabelle 2: Claude Duet im Vergleich zu den übrigen Claude-Angeboten

WICHTIG | Was Anthropic selbst einräumt

Duet ist ausdrücklich eine frühe Vorschau. Anthropic räumt ein, dass der Agent einen Mailverlauf falsch lesen oder die Dringlichkeit eines Vorgangs falsch einschätzen kann. Bei privaten Besorgungen – etwa Tickets buchen – ist er noch nicht sattelfest, und den Browser seiner virtuellen Maschine kannst du dir während der Preview nicht einmal ansehen. Für produktive Geschäftsprozesse ist das heute schlicht zu früh.

Was sind Chancen? Was sind Risiken?

Die Chancen

Man muss kein KI-Euphoriker sein, um das Potenzial zu sehen. Wer täglich 150 Mails, drei Kalender und ein halbes Dutzend Fachanwendungen jongliert, verliert erstaunlich viel Zeit mit Sortieren. Ein Agent, der vorsortiert und nur bei echten Entscheidungen stört, ist für Geschäftsführer kleiner Firmen, Vertrieb und Projektleitung ein echter Hebel.

- **Weniger Kontextwechsel:** Der Morgen-Brief ersetzt den Rundgang durch fünf Anwendungen.
- **Arbeit läuft weiter:** Recherchen, Entwürfe und Auswertungen werden fertig, während du im Termin sitzt.
- **Sauberes Freigabemodell:** Das Prinzip „vorbereiten ja, ausführen erst nach Okay“ taugt als Blaupause für jede Agenten-Richtlinie – egal ob Claude, Copilot oder Eigenbau.
- **Geringer Einführungsaufwand:** Wer Claude bereits mit Memory, Skills und Konnektoren nutzt, startet sofort.

Die Risiken

Das größte Risiko ist nicht die Technik, sondern der Weg, auf dem sie ins Unternehmen kommt. Solange es Duet nur für private Pläne gibt, gibt es keine Admin-Konsole, keine zentrale Konnektor-Steuerung und keinen Vertrag zur Auftragsverarbeitung, den die IT geprüft hätte. Ein Agent, der regelmäßig Firmenpostfächer liest, ist datenschutzrechtlich eine andere Hausnummer als ein Chat, dem man gelegentlich einen Text hineinkopiert.



Abbildung 3: Zwei Wege, wie proaktive Agenten ins Unternehmen kommen

WARNUNG | Der Vertriebsleiter und sein neuer Lieblingskollege

Ein typisches Szenario, wie es sich mit jeder neuen KI-Generation wiederholt: Der Vertriebsleiter liest über einen neuen Agenten, holt sich privat das passende Abo und verbindet „nur mal zum Testen“ Firmenpostfach, Kalender und CRM. Drei Wochen später schwärmt er im Jour fixe vom Morgen-Brief. Die IT erfährt davon, als die Geschäftsführung fragt, warum das nicht alle bekommen. Zu diesem Zeitpunkt hat der Agent bereits Hunderte Kundenmails, Angebote und Personalthemen verarbeitet –

ohne AV-Vertrag, ohne Protokoll, ohne Löschkonzept. Der Mann meinte es gut. Das Problem bleibt trotzdem deins.

Szenario	Empfehlung	Begründung
Mitarbeiter nutzen privat Pro oder Max mit Firmenkonten	Untersagen und über die Richtlinie aktiv ansprechen	Kein AV-Vertrag, keine Steuerung, kein Löschkonzept
Pilotgruppe will proaktive Agenten testen	Nur mit Testkonten und unkritischen Daten	Research Preview, Fehleinschätzungen ausdrücklich möglich
Duet kommt für Team und Enterprise	Bewertung wie jede neue KI-Komponente	Erst dann gibt es Admin-Kontrolle und Vertragsgrundlage
Unternehmen setzt bereits auf Microsoft 365 Copilot	Gleiche Agenten-Richtlinie für alle Anbieter	Proaktive Agenten kommen von allen Herstellern

Tabelle 3: Typische Szenarien und unsere Empfehlung

Was müssen wir jetzt schon vorbereiten?

Die gute Nachricht: Du musst nichts überstürzen. Die Vorlaufzeit bis zu einer Unternehmensversion ist ein Geschenk, das man nutzen sollte. Die meisten Bausteine brauchst du ohnehin – spätestens dann, wenn Microsoft, OpenAI oder Anthropic ihre proaktiven Agenten für Firmenkunden öffnen.

Was	Wer	Bis wann
Bestandsaufnahme: Wer nutzt privat Claude, ChatGPT, Muse und Co. mit Firmenkonten?	IT-Leitung, Informationssicherheit	kurzfristig
Richtlinie für proaktive Agenten: erlaubte Aufgaben, Datenklassen, Freigabepflichten	IT-Leitung, Datenschutzbeauftragter	vor der ersten Unternehmensversion
Positivliste für Konnektoren und Prüfung von Drittanwendungs-Zustimmungen im Mandanten	Identity-Team	laufend
Datenschutz und Mitbestimmung klären (AV-Vertrag, Drittlandtransfer, § 87 Abs. 1 Nr. 6 BetrVG)	Datenschutzbeauftragter, Betriebsrat	vor jedem Pilot
Pilotkonzept mit Testkonten und Erfolgskriterien	Fachbereich, IT	sobald Team oder Enterprise verfügbar ist

Tabelle 4: Vorbereitungsplan für proaktive Agenten

TIPP | Zustimmungen im Mandanten prüfen

Proaktive Agenten docken meist per OAuth an Mail und Kalender an. In Microsoft-365-Umgebungen lohnt deshalb ein Blick auf die Benutzerzustimmung für Drittanwendungen in Entra ID: Wer dort jedem Mitarbeiter erlaubt, beliebigen Apps Zugriff auf sein Postfach zu geben, hat die Tür für Schatten-Agenten schon sperrangelweit offen. Ein Admin-Zustimmungs-Workflow kostet einen Nachmittag und schließt sie.

Wie sich Claude generell sauber im Unternehmen einführen lässt, zeigt der Kompetenzbereich [Claude im Unternehmen](#). Und wenn du die Richtlinie für proaktive Agenten nicht allein stricken willst: Die [Beratung zu Claude und KI-Governance](#) startet mit einer KI-Standortbestimmung zum Festpreis.

Häufig gestellte Fragen

Gibt es Claude Duet in Deutschland?

Noch nicht. Die Research Preview steht aktuell nur Nutzern mit Pro- oder Max-Plan in den USA offen, und auch dort nur über eine Warteliste. Einen Termin für weitere Länder hat Anthropic nicht genannt.

Was kostet Claude Duet?

Einen eigenen Preis gibt es nicht. Duet verbraucht das Nutzungskontingent des bestehenden Claude-Plans – inklusive Morgen-Brief und Hintergrundprüfungen. Wer Duet intensiv arbeiten lässt, stößt entsprechend früher an die Grenzen seines Plans.

Ist Claude Duet DSGVO-konform?

Für den Unternehmenseinsatz lässt sich das derzeit nicht seriös bejahen, denn Duet gibt es nur für private Pläne ohne zentrale Verwaltung. Ein Agent, der regelmäßig Postfächer mit Kunden- und Personaldaten liest, braucht eine geprüfte Vertragsgrundlage, ein Löschkonzept und eine Bewertung des Drittlandtransfers. Das ist erst mit einer Unternehmensversion realistisch.

Kann Duet ohne meine Zustimmung Mails versenden oder bezahlen?

Nach Herstellerangabe nicht. Vor dem Senden von Nachrichten, Zahlungen, Unterschriften und Löschvorgängen fragt Duet nach. Passwörter sieht der Agent nicht direkt, und ein eigener Classifier soll verhindern, dass etwa Kartennummern weitergegeben werden. Die Schranke schützt allerdings nur so gut, wie der Mensch die Rückfragen tatsächlich liest.

Worin unterscheidet sich Duet von Microsoft 365 Copilot?

Copilot ist tief in den Microsoft-365-Mandanten integriert und läuft unter dessen Verwaltung, Berechtigungen und Compliance-Werkzeugen. Duet ist ein eigenständiger persönlicher Agent, der über Konnektoren an viele Dienste andockt und von sich aus aktiv wird. Für Unternehmen zählt am Ende weniger der Hersteller als die Frage, ob eine einheitliche Agenten-Richtlinie für alle Anbieter gilt.