● Included ▲ Included — Metered

		Microsoft 365 Copilot Chat Free + Consumption	Microsoft 365 Copilot $30 pupm
Chat	Copilot Chat – Web grounded (powered by GPT-4o)	●	●
	Copilot Chat – Work grounded (work data in your tenant's Microsoft Graph and 3rd party data via Graph connectors)		●
	Copilot Pages	●	●
	File upload[1]	●	●
	Code Interpreter[1]	●	●
	Image generation[1]	●	●
Agents[2]	Create agents using Copilot Studio[3], including SharePoint agents	●	●
	Discover and pin agents	●	●
	Use agents grounded in Web data	●	●
	Use agents grounded in work data (work data in your tenant's Microsoft Graph and 3rd party data via Graph connectors)	▲	●
	Use agents that act independently using autonomous actions	▲	▲
Personal assistant	Copilot reasons over personal work data (e.g., Outlook, OneDrive, Teams meeting transcripts and chats)		●
	Copilot in Teams		●
	Copilot in Outlook		●
	Copilot in Word		●
	Copilot in Excel		●
	Copilot in PowerPoint		●
	Copilot Actions		In preview
	Pre-built M365 agents (Interpreter, Facilitator, Project Manager, Employee Self-Service)		In preview
Copilot Control System	Enterprise Data Protection (EDP)	●	●
	IT management controls	●	●
	Agent management	●	●
	SharePoint Advanced Management		●
	Copilot Analytics to measure usage and adoption[4]		●
	Pre-built reports and advanced analytics to measure ROI		●

1. Limits apply. 2. Applies to employee-facing agents only. 3. Learn more about the full capabilities of Copilot Studio: aka.ms/CopilotStudioCapabilities 4. Basic reporting in Microsoft Admin Center available for Copilot Chat.

Upsell? Für den sicheren KI-Einsatz

M365 Business

Grundlegende Sicherheit

Copilot & M365 Business Standard

Multi-Faktor-Authentifizierung mit Sicherheitsstandards

Gerätebasierter Zugriff & Sicherheitskontrollen für M365-Ressourcen

Grundlegende Inhalts- und Stichwortsuche für Copilot-generierte Daten

Erstklassige Sicherheit

Copilot & Microsoft 365 Business Premium

Alles aus M365 Business Standard

plus:

Conditional Access Richtlinien basierend auf Identität, Gerät, Standort und Netzwerk

Terms of use policies zu akzeptieren, bevor Sie Zugriff erhalten

Einschränken des Speicherns von Geschäftsdaten und -dateien nur für genehmigte Anwendungen

Schutz sensibler M365-Daten vor Exfiltration und unsachgemäße Verwendung (nur Dateien und E-Mails)

eDiscovery, Beweissicherung und Aufbewahrung Richtlinien

O/ M365 Enterprise

Grundlegende Sicherheit

Copilot & Office 365 E3

Multi-Faktor-Authentifizierung mit Sicherheitsstandards

Manuelle Sensitivity Labels für Copilot-generierte Inhalte (Office only)

Erweiterte Sicherheit

Copilot & Microsoft 365 E3

Alles aus O365 E3

plus:

Conditional Access Richtlinien basierend auf Identität, Gerät, Standort und Netzwerk

Manuelle Sensitivity Labels für Microsoft und nicht Microsoft-Dokumente (z.B. pdf)

Endpoint Management

Erstklassige Sicherheit

Copilot & Microsoft 365 E5

Alles aus O & M365 E3

plus:

Benutzer-/Sitzungsrisiko und Access Control

Automatische Vertraulichkeitsbezeichnungen für Microsoft und nicht Microsoft-Dokumente (z.B. pdf)

Ermitteln und bewerten des Risiko von 400+ **KI-Apps** & **Implementieren** von **Kontrollen** für den Einsatz am Arbeitsplatz ...

Hinweis: Nicht alle Funktionen/Produkte werden angezeigt.

Entdecken – Kennen Sie Ihre Daten und verstehen Sie die Risiken?

Ermitteln Sie die potenziellen Daten- und Sicherheitsrisiken, die Microsoft 365 Copilot in Ihrem Unternehmen mit sich bringen könnte

Was ist sensibel?

Definieren Sie, was für die Organisation sensibel ist

Generisch & kundenspezifisch

- Betriebsgeheimnisse
- Streng vertraulich
- Personenbezogene Daten

Wo befinden sich die Daten?

Erstellung eines Inventars aller Datenrepositories

Gilt als Copilot-Quelle

- Microsoft 365
- 3rd party Quellen
- Strukturiert und unstrukturiert

Wer hat Zugriff?

Auf welche Inhalte können Mitarbeiter zugreifen?

Intern und extern innerhalb der Organisation

Zutrittskontrolle und Zutrittsmanagement

Oversharing

Wie wird es verwendet?

Übermäßige Offenlegung sensibler Daten Ungeschützte Daten

Wird die Verwendung sensibler Daten verwaltet??

Was ist das Risiko?

Was passiert, wenn Daten offengelegt werden?

Welche Daten könnten dem Unternehmen schaden?

Was wären die Auswirkungen und Kosten?

Sind wir gefährdet??

Sind wir compliant?

Organisatorische Risikotoleranz definiert die nächsten Schritte

Geringes Risiko
Aktiviere Copilot

Mittleres Risiko
Implementieren Sie (zusätzliche) Datensicherheit und aktivieren Sie parallel Copilot

Hohes Risiko
Implementieren Sie Datensicherheit, bevor Sie Copilot aktivieren

Schützen

Implementieren Sie Kontrollen, um Risiken zu mindern und zu reduzieren

Steuerelemente für den Datenlebenszyklus

Minimieren Sie veraltete Daten

Aufbewahrungsrichtlinien und automatisches Löschen

Records Management für geschäftliche, rechtliche oder behördliche Anforderungen an die Aufbewahrung von Aufzeichnungen

Datenschutz-Kontrollen

Verhindern Sie Datenverluste

Schutz vor übermäßiger und externer Freigabe

Schutz sensibler Informationen

- Datenverschlüsselung
- Wasserzeichen

Datenzugriffskontrollen

Zugriffsberechtigungen optimieren, entfernen, sperren

Korrektur oversharing

Ausschließen von Datenquellen

Kennzeichnung von Daten

Anwenden von Vertraulichkeitsbezeichnungen auf Daten

Manuell, vom Benutzer initiiert

Automatisch, basierend auf Inhalt, Ort, Zweck,etc.

Klassifizierung von Daten

Auswählen und Definieren von Typen vertraulicher Informationen

- Generisch, sofort einsatzbereit
- Kundenspezifisch, kundenspezifisch nach Spezifikation

Steigern Sie die Produktivität