

Sicherheit und Governance für Microsoft 365 Copilot

Schutz von Copilot mit
Microsoft Purview



Generative KI bringt neue Bedrohungen mit sich

Generative KI verändert die Arbeitswelt, schafft zugleich jedoch eine kontinuierlich wachsende KI-Bedrohungslandschaft mit kritischen Risikobereichen wie Datenlecks, neuen Bedrohungen und Schwachstellen sowie Compliance-Verstößen. Diese Bedrohungen verstärken bestehende Sicherheitsrisiken wie Datenverlust und Insider-Risiken. Sie führen auch neue Bedrohungen ein, wie z. B. Prompt-Injection-Angriffe und Urheberrechtsverletzungen.

90 %

der Unternehmen fehlen die Tools, um den heutigen KI-gestützten Bedrohungen zu begegnen.¹

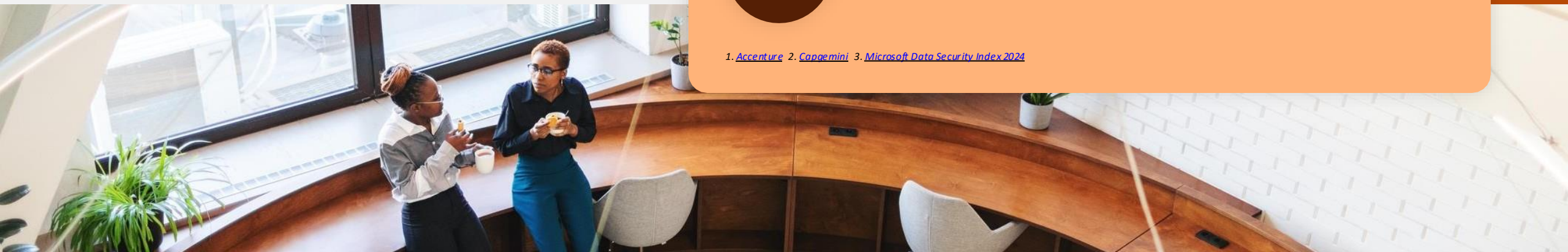
97 %

der Unternehmen haben Sicherheitsverletzungen im Zusammenhang mit der Nutzung generativer KI erlebt.²

84 %

aller Organisationen fehlt es an Vertrauen in die Verwaltung von Dateneingaben in KI Apps und Tools.³

1. [Accenture](#) 2. [Gartner](#) 3. [Microsoft Data Security Index 2024](#)



[ZURÜCK](#)

[WEITER](#)

Microsoft 365 Copilot mit KI: Sicherheit als Design

Kunden vertrauen Microsoft 365 Copilot ihre sensiblen Daten an. Microsoft 365 basiert auf einer sicheren und verantwortungsvollen KI und bietet branchenführende Sicherheits- und Governancefunktionen sowie Tools, um Unternehmen beim Risikomanagement zu unterstützen.

Microsoft 365 bietet zudem einen bewährten Ansatz für Datenschutz, der auf dem festen Versprechen basiert, Ihnen die Kontrolle über Ihre Daten zu ermöglichen.

Um Ihre Microsoft 365 Copilot-Daten verantwortungsbewusst verwalten und schützen zu können, müssen Sie riskante KI-Nutzung schnell identifizieren können, beispielsweise wenn ein Benutzer plötzlich auf eine große Menge sensibler Daten zugreift. Zusätzlich benötigen Sie Einblicke in Prompts und Antworten, um sicherzustellen, dass Sie die Nutzungsrichtlinien Ihres Unternehmens einhalten.



Minimieren von Risiken bei der Skalierung von Microsoft 365 Copilot

Microsoft 365 Copilot unterstützt Benutzer dabei, Inhalte basierend auf ihren Zugriffsberechtigungen zu erstellen.

Risiken zu minimieren heißt, über eine rein reaktive Aufsicht hinauszugehen und proaktive Governance zu etablieren. Dadurch wird sichergestellt, dass die Daten, die Microsoft 365 Copilot antreiben, konsistent verwaltet, angemessen gekennzeichnet und sicher geschützt werden.

Für die vollständige Absicherung und Governance von Microsoft 365 Copilot wird Folgendes benötigt:

Vermeiden von Datenlecks und zu weitreichenden Freigaben

Erkennen Sie potenzielle Risiken durch Oversharing und erhalten Sie umsetzbare Empfehlungen zu Richtlinien.

Riskante KI identifizieren

Schützen Sie vor Datenverlust und Insider-Risiken mit proaktiven Warnmeldungen und adaptivem Schutz.

KI-Governance und Risikotransparenz

Tragen Sie dazu bei, dass die Nutzung von Copilot und KI-Agenten den gesetzlichen Vorgaben, Unternehmensrichtlinien und ethischen Grundsätzen entspricht.



Eine vollständige Lösung für die Sicherheit und Governance von Microsoft 365 Copilot

Verschaffen Sie sich Transparenz über Risiken, erzwingen Sie Datenschutz und wenden Sie Governance-Kontrollen mit Microsoft Purview an.

Dieses umfassende Lösungspaket unterstützt Ihr Unternehmen dabei, Microsoft 365 Copilot-Daten in Ihrer gesamten Datenlandschaft zu steuern, zu schützen und zu verwalten. Eine einheitliche Ansicht bietet einen vereinfachten Ansatz für Ihre Datenschutzstrategie, der die Fragmentierung von Daten adressiert und die Einhaltung von Vorschriften sicherstellt.



So unterstützt Microsoft Purview Microsoft 365 Copilot:



Berücksichtigt
Oversharing von
Informationen



Schützt vor
Datenverlust und
Insider-Risiken



Steuert die
KI-Verwendung,
um Vorschriften und
Richtlinien einzuhalten



[ZURÜCK](#)

[WEITER](#)

Berücksichtigung von Oversharing von Informationen

Erkennen Sie potenzielle Risiken durch Oversharing und erhalten Sie umsetzbare Empfehlungen zu Richtlinien.



Microsoft Purview hilft Ihnen, potenziell zu weitreichend freigegebene Sites und Dateien in Ihrer gesamten Microsoft 365-Umgebung zu identifizieren.

Erhalten Sie Richtlinienvorschläge und wenden Sie diese an, um Ihre spezifischen Risiken durch zu weitreichende Freigaben zu minimieren. Entfernen Sie bei Bedarf den unternehmensweiten Site-Zugriff. Erhalten Sie Benachrichtigungen, wenn eine neue zu weitreichende Freigabe erfolgt, mit Optionen zur Behebung. Microsoft Purview schützt vertrauliche Dateien, unabhängig davon, wo sie gespeichert oder übertragen werden.



Wesentliche Funktionen:



Verhindern der Verarbeitung vertraulicher Daten



Korrektur von zu breiten Berechtigungen



Überblick über zu weitreichend freigegebene Inhalte



[ZURÜCK](#)

[WEITER](#)

Schutz vor Datenverlust und Insider-Risiken

Analysieren Sie Interaktionen mit sensiblen Daten, erhalten Sie Warnungen bei riskanten Aktivitäten und passen Sie Richtlinien risikobasiert dynamisch an.



Microsoft Purview verhindert Datenlecks, indem Sie Berichte über vertrauliche Daten und ungeschützte Dateien einsehen, Warnungen zu riskanter Nutzung erhalten und erkennen können, wenn Dateien vertrauliche Daten enthalten und automatisch Schutzmaßnahmen anwenden. Sie können Dateien auch dann schützen, wenn sie verschoben oder heruntergeladen werden. Und mit Microsoft Purview Insider-Risikomanagement können Sie den Zugriff für Benutzer mit hohem Risiko einschränken.

Wesentliche Funktionen:

Warnungen und
Berichte zu riskantem
Verhalten und KI-
Nutzung

Schutz vertraulicher
Dateien und
Interaktionen

Dynamische
Anwendung von
Sicherheitsrichtlinien
auf der Grundlage
riskanter Aktionen



[ZURÜCK](#)

[WEITER](#)



Steuern der KI-Verwendung, um Vorschriften und Richtlinien einzuhalten

Helfen Sie dabei sicherzustellen, dass die Nutzung von Microsoft 365 Copilot den Vorschriften wie dem EU-KI-Gesetz, den organisatorischen Richtlinien und den ethischen Grundsätzen entspricht.



Microsoft Purview hilft Ihnen, Interaktionen mit Microsoft 365 Copilot zu prüfen, indem Sie auf detaillierte Protokollinformationen zugreifen. Sie können Aufbewahrungs- und Löschrichtlinien für Interaktionen sowie Besprechungsaufzeichnungen und -transkripte erzwingen. Darüber hinaus erhalten Sie eine Warnung, wenn ein möglicher Compliance- oder Ethikverstoß auftritt, und Sie können eine Untersuchung einleiten.

Wesentliche Funktionen:



Überprüfung von Interaktionsinhalten und Überwachungsprotokollen



Untersuchung auf Compliance- und Ethikverstöße



Durchsetzung von Lebenszyklusrichtlinien und gesetzlichen Aufbewahrungsfristen



[ZURÜCK](#)

[WEITER](#)

Eine vollständige Lösung für die Sicherheit und Governance von Copilot



Microsoft Purview hilft Unternehmen, Microsoft 365 Copilot und Agenten sicher einzuführen und zu skalieren, indem es zu weitreichende Freigaben erkennt und verhindert, Datenverluste vermeidet und Governance durchsetzt, die auf die sich entwickelnden KI-Vorschriften abgestimmt ist.



„Wir nutzen Microsoft Purview, um sicherzustellen, dass von Copilot generierte Inhalte automatisch klassifiziert und geschützt werden, sodass ausschließlich autorisierte Benutzer Zugriff haben.“

—Manjunatha Sivanna, IT Service Delivery Manager, Cummins



[ZURÜCK](#)

[WEITER](#)



Mit der PROFI AG zu mehr Sicherheit

Als Microsoft-Partner sind wir bereit, Sie bei der Verteidigung Ihres Unternehmens vor Cyberbedrohungen zu unterstützen. Wir verfügen über eine solide Sicherheitspraxis und das Fachwissen, das Sie benötigen, um Sie in jeder Phase Ihrer Entwicklung zu unterstützen. Wir können eine Bewertung Ihrer aktuellen Umgebung vornehmen und die Lücken herausarbeiten sowie Ihnen bei der Umsetzung und Bereitstellung der bestmöglichen Sicherheitslösungen helfen, die auf Ihre individuellen Geschäftsanforderungen zugeschnitten sind.

Sichere
Copilot-
Einführung mit
klarer
Governance

Ganzheitlicher
Ansatz aus
Technik,
Security und
Adoption

Praxisnah &
passgenau für
Ihr
Unternehmen

Ihr Ansprechpartner: Jan Meyer-Böer
Geschäftsfeldleiter | Workplace Lösungen | PROFI AG
E-Mail: j.meyer-boeer@profi-ag.de
Telefon: +49 511 676885-3028



Sicherheit für die KI-Bewertung | Microsoft 365 Copilot

Sind Sie für Microsoft 365 Copilot bereit?

Bewerten Sie Ihre Sicherheits- und Governancebereitschaft und erhalten Sie maßgeschneiderte Empfehlungen, die Ihnen helfen, Ihre Microsoft 365-Umgebung vorzubereiten, Risiken zu erkennen und die Nutzung von Microsoft 365 Copilot zu schützen und zu verwalten.

[Mehr Erfahren](#)

Ressourcen

1

[Nutzung von Microsoft Purview zur Verwaltung von Datensicherheit und Compliance für Microsoft 365 Copilot und Microsoft 365 Copilot Chat](#)

2

[Microsoft Purview-Schutzmaßnahmen für Copilot](#)

3

[Oversharing-Kontrolle im Unternehmensmaßstab | Updates für Microsoft 365 Copilot mit Microsoft Purview](#)



[ZURÜCK](#)