Microsoft 365

KI-Potenzial erschließen – mit sicheren Grundlagen

Inhaltsverzeichnis

EINFÜHRUNG

KI-Chance und Sicherheitsimperativ

Es gibt eine wachsende Produktivitätskapazitätslücke der heutigen Arbeitswelt. Im aktuellen Work Trend Index-Bericht gaben **mehr als 80 %** der befragten Wissensarbeitenden (Mitarbeitende und Führungskräfte) aus 31 Ländern an, dass ihnen die Zeit oder Energie fehlt, um ihre Arbeit zu erledigen[1]. Gleichzeitig gaben **mehr als 50 %** der befragten Business-Führungskräfte an, dass die Produktivität gesteigert werden muss, um Ziele zu erreichen[1]. Dies bietet die Gelegenheit, unsere Arbeitsweise und mögliche Lösungen zu bewerten, um diese Lücke zu schließen. KI, einschließlich Agents, bietet vielversprechende Möglichkeiten als Lösung. **Mehr als 80 %** der befragten Führungskräfte waren zuversichtlich, dass ihre Unternehmen in den nächsten 12–18 Monaten KI-Agents einsetzen werden, um die Personalkapazität zu erweitern[1].

Dieser Ansturm auf KI geht jedoch mit einer Einschränkung einher: Innovation sollte mit robuster Sicherheit und Datenschutz in Einklang gebracht werden, um potenzielle Risiken zu minimieren. In einer aktuellen iSMG-Studie berichteten **mehr als 70 %** der befragten Business-Führungskräfte, dass sie die Gewährleistung von Datenschutz und Sicherheit die größte Herausforderung bei der Integration von generativer KI in die bestehende IT-Infrastruktur darstellt.[2] Führungskräfte stehen vor einem doppelten Imperativ: Sie müssen die KI-Einführung beschleunigen, um die Produktivität zu steigern, und gleichzeitig für Datenschutz in dieser neuen Ära sorgen.

Dieses E-Book bietet Einblicke in beispielhafte KI-Szenarien, die potenzielle Risiken bergen können, Tipps zur Risikominderung mit Microsoft 365 E3 sowie eine Checkliste, die Unternehmen dabei unterstützt, jetzt einzusteigen oder sich weiterhin auf die Einführung im großen Maßstab vorzubereiten. Bereiten Sie sich darauf vor, KI unbesorgt zu nutzen: Ermöglichen Sie Ihrem Unternehmen, mit KI Innovationen umzusetzen – ohne Kompromisse bei Sicherheits- oder Compliance-Standards einzugehen.

Gute Absichten mit potenziellen Risiken: KI-Beispielszenarien

Die größten Risiken bei der Nutzung und Einführung von KI entstehen häufig, wenn wohlmeinende Mitarbeitende versuchen, ihre Arbeit zu erledigen und eine größere Wirkung zu erzielen. Im Bestreben nach höherer Produktivität verarbeiten Teammitglieder möglicherweise unbeabsichtigt zu viele vertrauliche Informationen mit KI-Tools oder verwenden Anwendungen, die noch nicht von der IT genehmigt wurden. Dies kann zu Risiken führen und das Unternehmen neuen Bedrohungen aussetzen.

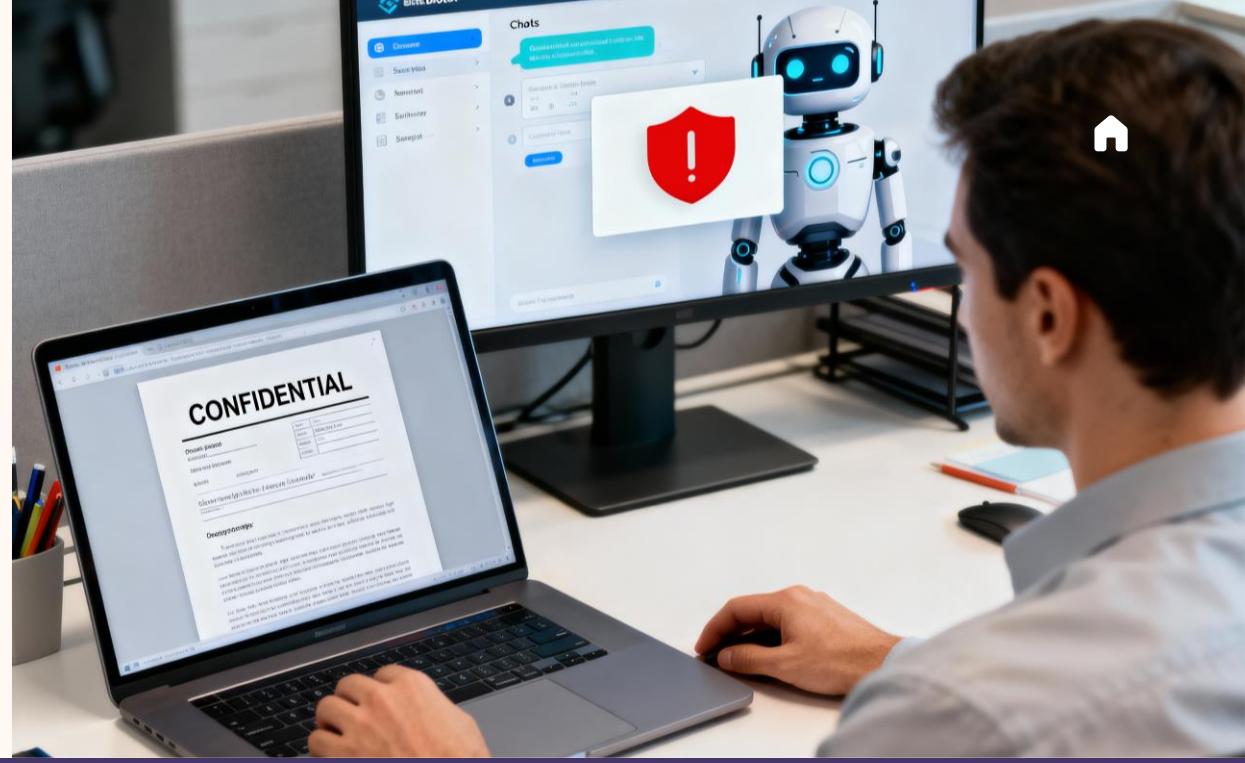
Sehen wir uns zur Verdeutlichung dessen zwei Beispielszenarien an – eines mit einem im Büro tätigen Informationsarbeiter und eines mit einer Fachkraft in Service und Produktion.

In diesen fiktiven Beispielen erfahren Sie 1), wie gut gemeinte KI-Nutzung zu Sicherheitsproblemen führen kann, wenn sie nicht richtig gesteuert wird, und 2), wie diese potenziellen Risiken mit einer robusten Sicherheitsgrundlage gemindert werden könnten.

Beispielszenario 1[4]

Ein Produktmarketing-Manager nutzt ein KI-Tool, um eine Pressemitteilung zu verfassen

Ein Produktmarketing-Manager in einem Fertigungsunternehmen steht unter hohem Zeitdruck, eine Pressemitteilung zu einem neuen Produkt zu verfassen, das in den kommenden Monaten eingeführt wird. Um Ideen zu sammeln und den Schreibprozess zu beschleunigen, kopiert dieser Mitarbeiter Auszüge aus einer vertraulichen Produkt-Roadmap und einer internen Finanzprognose und fügt sie in einen kostenlosen Online-KI-Schreibassistenten ein. Das KI-Tool erstellt schnell einige gut formulierte Absätze, die der Mitarbeiter anschließend im Entwurf der Pressemitteilung verwendet. Dieses Tool wurde jedoch noch nicht vom Unternehmen geprüft oder freigegeben.



Potenzielles Risiko:

Durch die Nutzung dieses externen KI-Diensts hat der Mitarbeiter sensible Unternehmensdaten (Produktpläne und Finanzinformationen) in ein Drittanbietersystem hochgeladen, in das das IT-Team keinen Einblick hat und das es weder verwalten noch kontrollieren kann. Sobald die Daten mit dem KI-Tool geteilt werden, verliert das Unternehmen die Kontrolle darüber, da sie sich außerhalb der genehmigten Grenzen befinden. Das Unternehmen kann nun nicht mehr nachvollziehen, wie lange die Daten gespeichert werden, wer Zugriff darauf hat oder wie sie von Drittanbietenden verwendet werden. Was als schneller Produktivitätsgewinn begann, ist zu einem Datenleck-Vorfall geworden. Dieses Szenario verdeutlicht das potenzielle interne Risiko, wenn wohlmeinende Mitarbeitende sensible Daten an ein nicht genehmigtes KI-Tool übertragen und dadurch das Unternehmen angreifbar machen.

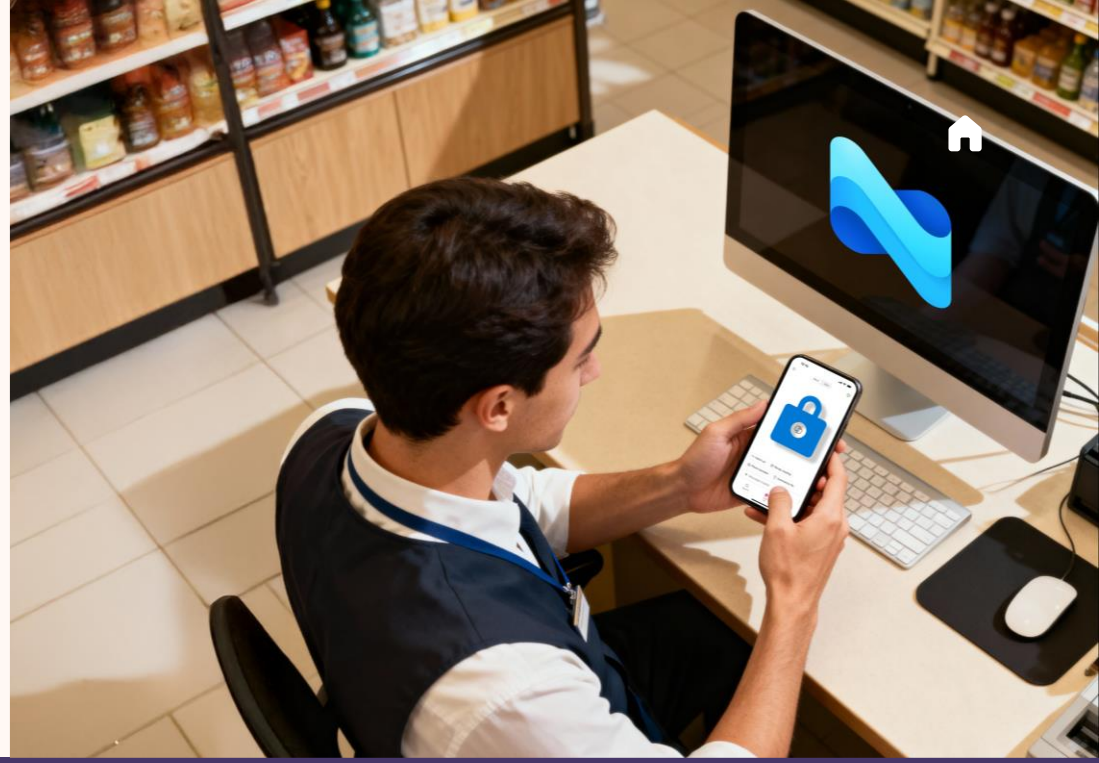
Risikominderung mit Microsoft 365 E3:

Microsoft 365 E3 bietet verschiedene Funktionen und Fähigkeiten, die dazu beitragen können, dieses Ergebnis zu verhindern. **Microsoft Purview Information Protection Plan 1** ermöglicht Ihnen, Vertraulichkeitsbezeichnungen und Verschlüsselung auf Dokumente anwenden, z. B. auf die Produkt-Roadmap und Finanzprojektdokumente. Wären diese Dokumente mit Vertraulichkeitsbezeichnungen wie *Vertraulich* und Verschlüsselung klassifiziert und verschlüsselt worden, hätte der Zugriff auf die Dokumente auf ausschließlich autorisierte Benutzende beschränkt werden können. Zusätzlich kann **Cloud App Discovery** dabei helfen, GenAI-Cloud-Apps zu identifizieren, die verwendet werden (von den vielen Apps im Cloud-App-Katalog), einschließlich des jeweiligen Nutzers und der Nutzungsfrequenz. Die IT-Abteilung hätte feststellen können, dass Mitarbeitende dieses spezielle KI-Tool verwendeten, und entsprechende Maßnahmen ergreifen können, um dessen Nutzung mit **Microsoft Defender for Endpoint P1** einzuschränken oder eine genehmigte Alternative bereitzustellen. Microsoft 365 E3 bietet die Tools und Funktionen, mit denen Unternehmen die Transparenz verbessern und Risiken mindern können.

Beispielszenario 2[4]

Ein Filialleiter verwendet KI, um Mitarbeiterpläne und Notizen zur Leistung zu erstellen

Ein Filialleiter einer großen Einzelhandelskette ist mit administrativen Aufgaben überfordert und entdeckt eine kostenlose KI-Produktivitäts-App, die verspricht, bei der Planung und Dokumentation zu helfen. Um Zeit zu sparen, importiert der Filialleiter eine Tabelle mit Mitarbeiternamen, Telefonnummern, Stundenlöhnen, Verfügbarkeitspräferenzen und aktuellen Leistungsnotizen in das KI-Tool. Er weist die KI-App an, einen optimierten Arbeitsplan zu erstellen und dabei zu helfen, Zusammenfassungen von Leistungsbeurteilungen zur Vorbereitung bevorstehender Einzelgespräche zu entwerfen.



Potenzielles Risiko:

Durch das Hochladen dieser Mitarbeiterdaten in eine ungeprüfte KI-App hat der Filialleiter sensible personenbezogene Daten seiner Mitarbeitenden über ein Drittanbietersystem offengelegt, das sich der Kontrolle und Aufsicht des Unternehmens entzieht. Dies könnte zu potenziellen Datenschutzverletzungen und Compliance-Problemen mit Arbeitsgesetzen führen. Die Personal- und IT-Abteilungen des Unternehmens haben keinen Einblick darin, an welchem Speicherort sich die Mitarbeiterdaten jetzt befinden, wie lange sie gespeichert werden oder wer darauf zugreifen kann. Was als Versuch begann, effizienter zu sein, führte zu erheblichen Problemen in Bezug auf rechtliche Fragen, Datenschutz und Mitarbeitervertrauen.

Risikominderung mit Microsoft 365 E3:

Die Geräte- und Anwendungsverwaltungsfunktionen von Microsoft 365 E3 können dazu beitragen, Risiken wie diese in Service und Produktion zu mindern. Mit **Microsoft Intune P1** könnte das IT-Team des Einzelhändlers Anwendungsschutzrichtlinien erzwingen, um Regeln auf Anwendungen anzuwenden, die auf Geschäftsdaten zugreifen, und z. B. das Kopieren/Einfügen und die Datenübertragung zu nicht verwalteten Apps zu unterbinden. Wenn der Einzelhändler Richtlinien für bedingten Zugriff über **Microsoft Entra ID P1** erstellt, kann er möglicherweise verhindern, dass sich Benutzende von nicht verwalteten Apps oder Geräten bei Unternehmenskonten anmelden. In diesem Szenario können diese Richtlinien verhindern, dass der Manager mit einem nicht konformen Telefon oder einer nicht verwalteten App auf eingeschränkte Unternehmensdateien zugreift und sie in eine Schatten-KI-Anwendung hochlädt.

WICHTIGE ERKENNTNIS: In beiden Szenarien verfolgten die Mitarbeiter ein positives Ziel – die Arbeitseffizienz mithilfe von KI zu verbessern. Das Ergebnis könnte jedoch negativ ausfallen, wenn keine geeigneten Schutzmechanismen und Richtlinien vorhanden sind. Diese Beispiele verdeutlichen, warum die Einführung von KI ohne ein Sicherheitsnetz neue und zusätzliche Risiken für Unternehmen mit sich bringen kann. Ziel ist es nicht, den Einsatz von KI zu verhindern, sondern ihn verantwortungsvoll zu ermöglichen. Im nächsten Abschnitt werden die grundlegenden Fähigkeiten vorgestellt, die bei der Bewertung von Lösungen zur Verbesserung der Produktivitätskapazität zu berücksichtigen sind. Außerdem werden die Microsoft 365 E3-Funktionen erläutert, mit denen Unternehmen Schutzmechanismen einrichten können, damit sensible Daten in genehmigten, sicheren Kanälen bleiben.

Aufbau einer sicheren, KI-fähigen Grundlage mit Microsoft 365 E3

Ist Ihr Unternehmen bereit für die Skalierung von KI? Sehen Sie sich die folgende Checkliste an, und erfahren Sie, wie Microsoft 365 E3 Ihnen dabei helfen kann.

Mit der zunehmenden Einführung von KI wird es immer wichtiger, den Sicherheitsstatus Ihres Unternehmens zu bewerten und potenzielle Lücken zu identifizieren, bevor Sie KI skalieren. Microsoft 365 E3 wurde als KI-fähige Produktivitäts- und Sicherheitsgrundlage entwickelt und vereint eine breite Palette von Identitäts-, Sicherheits-, Compliance- und Verwaltungstools, die zusammenarbeiten, um Ihnen zu ermöglichen, Ihre KI-Einführung zuverlässig zu skalieren.

Verwenden Sie die folgende Checkliste als Ausgangspunkt, um den aktuellen Stand Ihres Unternehmens zu verstehen. Wenn bestimmte Maßnahmen noch nicht vollständig implementiert sind, könnte Ihr Unternehmen unnötigen Risiken ausgesetzt sein.

Setzen Sie starke Richtlinien für Identitäts- und Zugriffsverwaltung durch, wie Multi-Faktor-Authentifizierung (MFA) und bedingten Zugriff.

Microsoft 365 E3 enthält **Microsoft Entra ID P1**, wodurch die Durchsetzung einer robusten Identitäts- und Zugriffsverwaltung sowohl in der Cloud als auch in On-Premises-Umgebungen ermöglicht wird. Lösungen wie MFA und Richtlinien für bedingten Zugriff verifizieren jede Anmeldung und gewähren oder verweigern den Zugriff basierend auf Kriterien wie Benutzerrolle, Geräteintegrität und Standort, wodurch unbefugter Zugriff und übermäßige Weitergabe von Daten eingedämmt werden. Sie könnten beispielsweise den Zugriff auf KI-Anwendungen auf bestimmte Mitarbeitergruppen beschränken und für die Anmeldung die Multi-Faktor-Authentifizierung (MFA) vorschreiben, wodurch das Risiko einer Kontokompromittierung reduziert wird. Richtlinien für bedingten Zugriff können sensible Daten zusätzlich schützen, indem sie verhindern, dass Mitarbeitende mit Unternehmensanmeldedaten auf nicht genehmigte Anwendungen zugreifen. Außerdem können gemeinsam genutzte Geräte Abmelderegeln durchsetzen, um vor unbefugter Nutzung von Sitzungen zu schützen.

Ermöglichen Sie sichere Zusammenarbeit über verwaltete Endpunkte und Geräte hinweg.

Microsoft 365 E3 bietet intelligente Endpunktsicherheit durch Lösungen wie **Intune P1, Defender for Endpoint P1 und Windows E3**. Diese Tools ermöglichen die Verwaltung und Verbesserung der Sicherheit von PCs, mobilen Geräten und Apps. Unternehmen können Webfilterung durchsetzen, um riskante Websites (einschließlich nicht genehmigter KI-Tools) zu blockieren und Geräte mit Sicherheitspatches über **Windows Autopatch und Autopilot** zu aktualisieren. Diese Kontrollen tragen dazu bei, dass Geräte sicher, verwaltet und mit Sicherheitspatches auf dem neuesten Stand sind, wodurch die Angriffsfläche reduziert wird. Einheitliches Endpunkt- und Geräteverwaltung ermöglicht es Unternehmen, Arbeitsgeräte abzusichern und die Compliance von Anwendungen sicherzustellen – unabhängig davon, ob Mitarbeitende ihre eigenen oder vom Unternehmen bereitgestellte Geräte verwenden.

Schützen Sie Daten mithilfe von Funktionen wie Vertraulichkeitsbezeichnung und Richtlinien zur Verhinderung von Datenverlust.

Microsoft 365 E3 bietet grundlegende **Purview**-Funktionen – Vertraulichkeitsbezeichnung, Verschlüsselung und Verhinderung von Datenverlust (DLP) – zum Schutz sensibler Informationen in Dokumenten und E-Mails. Sobald Bezeichnungsrichtlinien veröffentlicht sind, können Mitarbeitende Dateien mit Finanzdaten, personenbezogenen Informationen oder geistigem Eigentum klassifizieren (zum Beispiel mit der Bezeichnung „Vertraulich“) und anschließend Verschlüsselung sowie Zugriffssteuerung anwenden. DLP-Richtlinien können unbefugte Freigaben über **Exchange Online und SharePoint Online/OneDrive for Business** erkennen und einschränken. Auch bei Verwendung von **Microsoft 365 Copilot** bleiben diese Schutzmaßnahmen bestehen: Copilot respektiert die höchste Vertraulichkeitsbezeichnung und verhindert, dass Benutzende ohne entsprechende Berechtigung auf geschützten Inhalt zugreifen oder diesen analysieren können.

Erhalten Sie Einblick in die Verwendung von nicht genehmigten KI-Tools, und ergreifen Sie fundierte Maßnahmen.

Microsoft 365 E3 enthält **Cloud App Discovery**, das Ihnen hilft zu erkennen, welche KI-Anwendungen verwendet werden (von den im Cloud-App-Katalog enthaltenen), von wem und mit welchen Risikobewertungen, sodass Sie auf Basis dieser Informationen entsprechende Maßnahmen ergreifen können. Falls als zu riskant eingestuft, kann die IT **Defender for Endpoint P1** verwenden, um den Zugriff einzelner Benutzer auf eine bestimmte URL auf verwalteten Windows 11-Geräten zu beschränken. Wenn Sie beispielsweise feststellen, dass 100 Benutzende ein bestimmtes KI-Bildgenerator-Tool verwenden, das weder geprüft noch freigegeben wurde, kann die IT es gemäß den Sicherheits- und Compliance-Standards Ihres Unternehmens untersuchen. Wenn es als riskant eingestuft wird, kann die IT eine offiziell freigegebene Alternative vorschlagen. Diese Funktionen versetzen Sie in die Lage, Risiken durch Schatten-KI zu mindern und fundierte Entscheidungen hinsichtlich der Nutzung von KI zu treffen, die zu Ihrem Unternehmen passen.

Stellen Sie zugelassene KI-Anwendungen wie Microsoft 365 Copilot bereit.

Die Bereitstellung zugelassener KI-Anwendungen bietet erheblichen Mehrwert, indem sie Mitarbeitenden Zugang zu leistungsstarken, genehmigten Tools verschafft, die den Sicherheits- und Compliance-Standards Ihres Unternehmens entsprechen. Anstatt dass Mitarbeitende beispielsweise auf ungeprüfte KI-Bildgeneratoren oder Chatbots zurückgreifen, kann die IT offiziell freigegebene Alternativen – wie **Microsoft 365 Copilot** – bereitstellen, die überwacht, unterstützt und in die bestehenden Unternehmensrichtlinien integriert sind. **Microsoft 365 Copilot** bietet eine sichere KI-Lösung der Enterprise-Klasse, die nahtlos in die Microsoft 365-Produktivitäts-Suite integriert ist. **Copilot** ermöglicht es Mitarbeitenden, intelligenter zu arbeiten, Routineaufgaben zu automatisieren und Insights zu generieren – und das alles unter Einhaltung von Identitäts- und Datenschutzrichtlinien. Dieser Ansatz reduziert Schatten-IT, hilft, Datenlecks zu begrenzen, und verschafft Unternehmen Transparenz und Kontrolle darüber, wie KI eingesetzt wird.

Diese Schutzmechanismen arbeiten nicht isoliert – sie verstärken sich gegenseitig als integrierte, mehrschichtige Verteidigung. Identitäts-, Geräte- und Datenschutzrichtlinien greifen ineinander, um Sie bei der Abwehr von Bedrohungen zu unterstützen. Wenn Sicherheitsteams wissen, dass solche Kontrollen vorhanden sind, kann Sicherheit zum Motor für Innovationen statt zum Hemmnis werden.

Microsoft 365 E3 unterstützt Sie dabei, die richtigen Schutzmaßnahmen einzurichten, damit Ihr Unternehmen mit KI innovativ sein kann, ohne Kompromisse bei der Sicherheit einzugehen.

Setzen Sie Ihren Weg zu KI fort

Jedes Unternehmen befindet sich auf einer Reise, um herauszufinden, wie KI seine Ziele am besten unterstützen kann. Das Versprechen ist verlockend – aber die Einführung von KI muss Hand in Hand mit einem robusten Schutz gehen. Mit Microsoft 365 E3 müssen Sie sich nicht zwischen beiden Optionen entscheiden. Sie erhalten eine leistungsstarke Suite, die Ihren Sicherheits- und Compliance-Status erhöht und es Ihnen ermöglicht, KI unbesorgt zu nutzen.

Bewerten Sie Ihre KI-Sicherheits-Readiness.

Microsoft bietet eine **Sicherheitsbewertung für KI**[3]. Diese Online-Bewertung (unter security-for-ai-assessment.microsoft.com) bietet Empfehlungen zur Verbesserung Ihrer KI-Sicherheit basierend auf den von Ihnen bereitgestellten Informationen. Sie hilft Ihnen, Ihre aktuelle KI-Sicherheit anhand der vier zentralen Säulen: **Vorbereiten**, **Entdecken**, **Schützen** und **Steuern** sowie durch umsetzbare Empfehlungen zu bewerten.

Erfahren Sie mehr, und nehmen Sie Kontakt mit Microsoft auf.

Informieren Sie sich über die Funktionen von Microsoft 365 E3 und wie diese Sie bei der sicheren Einführung von KI unterstützen: www.microsoft.com/en-us/microsoft-365/enterprise/e3?activetab=pivot:overviewtab. Sie können sich auch an Ihr Microsoft-Kundenbetreuerteam oder Ihren Microsoft-Partner wenden.

1. Work Trend Index-Jahresbericht, 2025: The Year the Frontier Firm Is Born Microsoft, Inc., April 2025. Microsoft analysierte zwischen dem 6. Februar und dem 24. März 2025 Umfragedaten von 31.000 Vollzeitbeschäftigten oder selbstständigen Wissensarbeitenden in 31 Ländern, LinkedIn-Arbeitsmarkttrends sowie Billionen von Microsoft 365-Produktivitätssignalen.
2. Second Annual Generative AI Study: Business Rewards vs. Security Risks, iSMG, Inc., Februar 2025 – basierend auf einer Umfrage unter mehr als 360 Geschäftsleuten und Cybersicherheitsfachkräften, durchgeführt im 3. Quartal 2024.
3. Sicherheitsbewertung für KI: security-for-ai-assessment.microsoft.com/ Die Genauigkeit der Ergebnisse hängt von der Genauigkeit Ihrer Eingabe ab. Der Bericht dient ausschließlich zu Website ab. Informationszwecken. Es werden weder Leistungen noch Ergebnisse garantiert. Der Bericht sollte nicht als Zusage von Microsoft verstanden werden. Die tatsächlichen Ergebnisse können je nach Standort, Kaufmethode und Nutzung abweichen. Microsoft gibt keine ausdrückliche oder konkludente Gewährleistung hinsichtlich des Inhalts dieses Berichts oder dieser
4. Die dargestellten Szenarien sind fiktiv und dienen nur zur Veranschaulichung.