Microsoft 365

Zbuduj bezpieczne fundamenty pod rozwój AI

Zawartość

WSTĘP

Potencjał AI i imperatyw bezpieczeństwa

Wśród dzisiejszego personelu rośnie luka w zakresie potencjału produktywności. W najnowszym raporcie Work Trend Index **ponad 80 proc.** pracowników umysłowych ankietowanych w 31 krajach — w tym pracownicy i liderzy — stwierdziło, że nie ma czasu lub energii na wykonywanie swojej pracy[1]. Jednocześnie **ponad 50 proc.** ankietowanych liderów biznesowych uznało, że zwiększenie produktywności jest konieczne, aby osiągnąć cele[1]. To stwarza okazję do przeanalizowania sposobów, w jakie pracujemy, oraz potencjalnych rozwiązań, które mogą pomóc zlikwidować tę lukę. Technologia AI, w tym agenty, stanowi obiecujące rozwiązanie. **Ponad 80 proc.** ankietowanych liderów wyraziło przekonanie, że ich organizacje zaczną korzystać z agentów AI w celu zwiększenia potencjału kadrowego w ciągu najbliższych 12–18 miesięcy[1].

Ten pośpiech w kierunku AI wiąże się z pewnym zastrzeżeniem: innowacyjność powinna iść w parze z niezawodnym bezpieczeństwem i ochroną danych, aby ograniczyć potencjalne ryzyko. W ostatnim badaniu iSMG **ponad 70 proc.** ankietowanych liderów biznesowych stwierdziło, że zapewnienie prywatności i bezpieczeństwa danych jest głównym wyzwaniem podczas integrowania generatywnej AI z istniejącą infrastrukturą IT[2]. Liderzy stoją przed podwójnym imperatywem: przyspieszenie wdrażania AI, aby zwiększyć produktywność i chronić dane w nowej erze pracy.

Ten e-book zawiera informacje na temat przykładowych scenariuszy AI, które mogą wiązać się z potencjalnymi zagrożeniami, wskazówki dotyczące ich ograniczania za pomocą Microsoft 365 E3 oraz listę kontrolną, która pomagają organizacjom rozpocząć lub kontynuować przygotowania do wdrożenia AI na dużą skalę. Przygotuj się, aby pewnie wdrażać AI: umożliwiając Twojej organizacji wprowadzanie innowacji z wykorzystaniem AI bez naruszania zabezpieczeń lub standardów zgodności.

Dobre intencje a potencjalne ryzyko: przykładowe scenariusze AI

Największe zagrożenia związane z wykorzystaniem i wdrażaniem AI często wynikają z działań pracowników o dobrych intencjach, którzy starają się wykonywać swoją pracę i osiągać lepsze rezultaty. W dążeniu do zwiększenia produktywności członkowie zespołu mogą przypadkowo ujawniać informacje wrażliwe narzędziom AI lub korzystać z aplikacji, które nie zostały jeszcze zatwierdzone przez dział IT. Może to stwarzać ryzyko i narażać organizację na nowe zagrożenia.

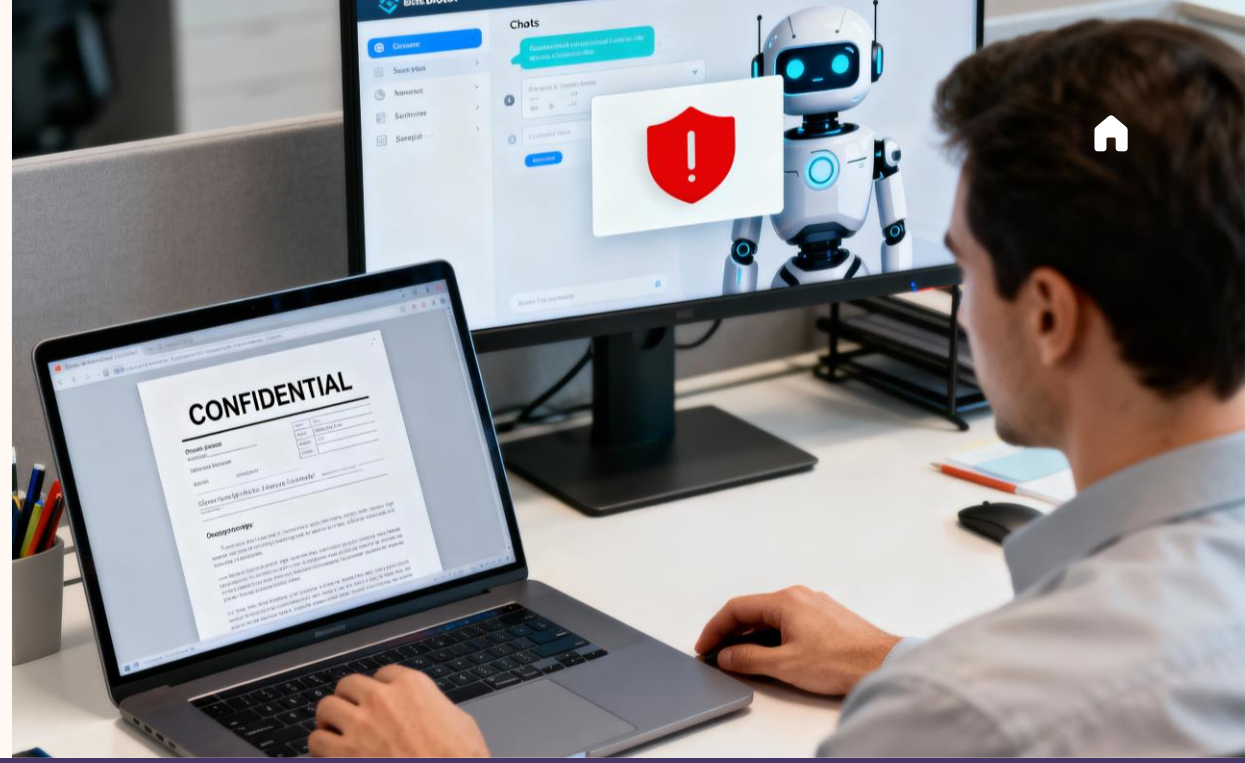
Przyjrzyjmy się dwóm przykładowym scenariuszom, aby zilustrować ten punkt — jeden z pracownikiem biurowym, a drugi z pracownikiem pierwszego kontaktu.

Z tych fikcyjnych przykładów dowiesz się: 1) jak użycie AI w dobrej wierze może prowadzić do naruszenia zabezpieczeń, jeśli nie jest odpowiednio zarządzane; oraz 2) jak można ograniczyć potencjalne zagrożenia dzięki solidnym fundamentom bezpieczeństwa.

Przykładowy scenariusz 1[4]

Menedżer ds. marketingu produktu wykorzystuje narzędzie AI do przygotowania wersji roboczej komunikatu prasowego

Menedżer ds. marketingu produktu w firmie produkcyjnej ma napięty termin na przygotowanie wersji roboczej komunikatu prasowego dotyczącego nowego produktu, którego premiera odbędzie się w najbliższych miesiącach. Aby zebrać pomysły i przyspieszyć proces pisania, pracownik kopiuje i wkleja fragmenty poufnego planu rozwoju produktu oraz wewnętrznej prognozy finansowej do bezpłatnego internetowego asystenta pisania opartego na AI. Narzędzie AI szybko generuje dopracowane akapity, które pracownik wykorzystuje następnie w wersji roboczej komunikatu prasowego. Narzędzie to nie zostało jednak jeszcze sprawdzone ani zatwierdzone przez organizację.



Potencjalne ryzyko:

Korzystając z tego zewnętrznego narzędzia AI, pracownik przesłał poufne dane firmy (plany produktu i informacje finansowe) do systemu zewnętrznego, do którego zespół IT nie ma wglądu, którym nie może zarządzać ani którego nie może kontrolować. Po udostępnieniu danych narzędziu AI firma traci nad nimi kontrolę, ponieważ wykraczają one poza dozwolone granice. Organizacja nie ma teraz informacji, jak długo dane są przechowywane, kto ma do nich dostęp ani w jaki sposób są wykorzystywane przez osobę trzecią. To, co początkowo było szybkim usprawnieniem pracy, przerodziło się w incydent obejmujący wyciek danych. Ten scenariusz odzwierciedla potencjalne ryzyko wewnętrzne, gdy pracownik z dobrymi intencjami udostępnia dane wrażliwe nieautoryzowanemu narzędziu AI, narażając organizację na ryzyko.

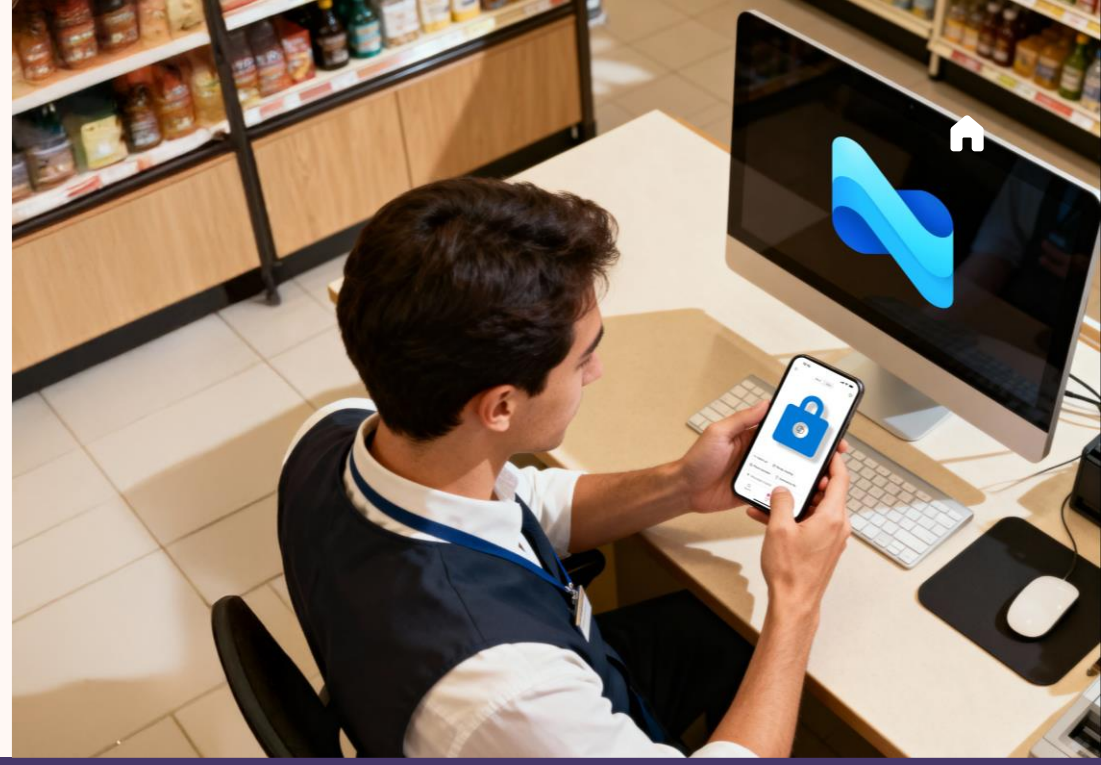
Ograniczanie ryzyka dzięki Microsoft 365 E3:

*Microsoft 365 E3 oferuje szereg funkcji i rozwiązań, które mogą pomóc zapobiec takiej sytuacji. * **Microsoft Purview Information Protection Plan 1** pozwala stosować etykiety poufności i szyfrowanie do dokumentów, takich jak plan rozwoju produktu czy dokumenty finansowe projektów. Gdyby te dokumenty zostały sklasyfikowane i zaszyfrowane przy użyciu etykiet poufności, takich jak *Poufne*, dostęp do nich mogliby mieć wyłącznie użytkownicy autoryzowani. Dodatkowo rozwiązanie **Cloud App Discovery** może pomóc zidentyfikować aplikacje generatywnej AI w chmurze, które są używane (spośród wielu aplikacji w wykazie aplikacji w chmurze), przez którego użytkownika i jak często. Zespół IT mógł wykryć, że pracownicy korzystali z tego konkretnego narzędzia AI i podjąć działania ograniczające jego użycie za pomocą usługi **Ochrona punktu końcowego w usłudze Microsoft Defender P1** lub zapewnić zatwierdzoną alternatywę. Microsoft 365 E3 zapewnia narzędzia i możliwości, które pomagają organizacjom zwiększyć widoczność i ograniczyć ryzyko.

*Przykładowy scenariusz 2[4]

Menedżer sklepu detalicznego wykorzystuje AI do tworzenia grafików pracy pracowników i notatek dotyczących ich wyników

Menedżer sklepu dużej sieci handlu detalicznego jest przytłoczony zadaniami administracyjnymi i odkrywa bezpłatną aplikację biurową opartą na AI, która obiecuje pomóc mu w planowaniu grafików i sporządzaniu dokumentacji. Aby zaoszczędzić czas, menedżer przesyła do narzędzia AI arkusz kalkulacyjny zawierający imiona i nazwiska pracowników, numery telefonów, stawki godzinowe, preferencje dotyczące dyspozycyjności oraz ostatnie notatki dotyczące wyników. Prosi aplikację AI o stworzenie zoptymalizowanego harmonogramu pracy oraz pomoc w przygotowaniu podsumowań ocen okresowych na nadchodzące spotkania indywidualne.



Potencjalne ryzyko:

Przesyłając te dane pracowników do niesprawdzonej aplikacji AI, menedżer ujawnił poufne dane osobowe swoich pracowników systemowi zewnętrznemu, który znajduje się poza kontrolą i nadzorem firmy. Może skutkować naruszeniem prywatności i niezgodnością z przepisami prawa pracy. Działy kadr i IT firmy nie mają wglądu w to, gdzie obecnie znajdują się dane pracowników, jak długo są przechowywane ani kto może mieć do nich dostęp. To, co miało zwiększyć efektywność, doprowadziło do poważnych problemów prawnych, dotyczących prywatności oraz zaufania pracowników.

Ograniczanie ryzyka dzięki Microsoft 365 E3:

Możliwości zarządzania urządzeniami oraz aplikacjami w Microsoft 365 E3 mogą pomóc w ograniczaniu ryzyka związanego ze scenariuszami obejmującymi pracowników pierwszego kontaktu. Dzięki **Microsoft Intune P1** zespół IT sprzedawcy detalicznego może egzekwować zasady ochrony aplikacji, aby stosować reguły do aplikacji mających dostęp do danych służbowych, np. ograniczać kopiowanie, wklejanie i przesyłanie danych do niezarządzanych aplikacji. Jeśli firma utworzy zasady dostępu warunkowego za pomocą usługi **Microsoft Entra ID P1**, może zablokować próby logowania do kont służbowych z niezarządzanych aplikacji lub urządzeń. W tym scenariuszu, jeśli telefon menedżera nie jest zgodny z wymaganiami lub aplikacja jest niezarządzana, te zasady mogą pomóc uniemożliwić mu dostęp do zastrzeżonych plików firmowych oraz ich przesyłanie do niezatwierdzonej (shadow) aplikacji AI.

KLUCZOWE WNIOSKI: W obu scenariuszach intencje pracowników były pozytywne — poprawa efektywności pracy dzięki AI. Skutki mogą być jednak negatywne, jeśli nie zostaną wdrożone odpowiednie zabezpieczenia i zasady. Te przykłady pokazują, dlaczego wdrażanie AI bez odpowiednich zabezpieczeń może wiązać się z nowymi i dodatkowymi zagrożeniami dla organizacji. Ich celem nie jest zniechęcanie do korzystania z AI, lecz skoncentrowanie się na jej odpowiedzialnym użyciu. W następnej sekcji omówione zostaną podstawowe możliwości, które należy wziąć pod uwagę przy ocenie rozwiązań mogących zwiększyć wydajność, oraz możliwości Microsoft 365 E3, które pomagają organizacjom wdrażać zabezpieczenia chroniące dane wrażliwe w zatwierdzonych, bezpiecznych kanałach.

Budowanie bezpiecznych podstaw gotowych na AI dzięki Microsoft 365 E3

Czy Twoja organizacja jest gotowa do skalowania AI? Zapoznaj się z poniższą listą kontrolną i dowiedz się, jak Microsoft 365 E3 może pomóc Twojej organizacji.

Wraz z przyspieszeniem wdrażania AI coraz ważniejsza staje się ocena stanu zabezpieczeń organizacji i identyfikowanie potencjalnych luk przed skalowaniem AI. Pakiet Microsoft 365 E3 został zaprojektowany jako gotowa na AI podstawa zapewniająca produktywność i bezpieczeństwo — łącząc szeroki zakres narzędzi do obsługi tożsamości, bezpieczeństwa, zgodności i zarządzania, które współpracują ze sobą, aby umożliwić Ci pewne skalowanie wdrożenia AI.

Użyj poniższej listy kontrolnej jako punktu wyjścia do oceny aktualnego stanu Twojej organizacji. Jeśli pewne elementy nie zostały jeszcze w pełni wdrożone, Twoja organizacja może być narażona na niepotrzebne ryzyko.

Stosuj rygorystyczne zasady zarządzania tożsamościami i dostępem, obejmujące uwierzytelnianie wieloskładnikowe (MFA) i dostęp warunkowy.

Microsoft 365 E3 obejmuje usługę **Microsoft Entra ID P1**, która umożliwia egzekwowanie zaawansowanych zasad zarządzania tożsamościami i dostępem zarówno w środowiskach chmurowych, jak i lokalnych. Rozwiązania, takie jak uwierzytelnianie wieloskładnikowe (MFA) i zasady dostępu warunkowego, weryfikują każde logowanie oraz ograniczają lub zezwalają na dostęp w oparciu o kryteria, takie jak rola użytkownika, kondycja urządzenia i lokalizacja, pomagając ograniczyć nieautoryzowany dostęp i nadmierne udostępnianie danych. Można na przykład ograniczyć dostęp do aplikacji AI do określonych grup pracowników i wymagać uwierzytelniania wieloskładnikowego podczas logowania, zmniejszając w ten sposób ryzyko naruszenia zabezpieczeń konta. Zasady dostępu warunkowego mogą dodatkowo chronić dane wrażliwe, uniemożliwiając pracownikom dostęp do aplikacji niezaakceptowanych oficjalnie przy użyciu firmowych danych logowania, a urządzenia współdzielone mogą egzekwować reguły wylogowywania, aby zapobiec nieautoryzowanemu korzystaniu z sesji.

Zapewnij bezpieczną współpracę na zarządzanych urządzeniach klienckich i innych.

Microsoft 365 E3 oferuje inteligentne zabezpieczenia urządzeń klienckich dzięki rozwiązaniom, takim jak **Intune P1, Ochrona punktu końcowego w usłudze Defender P1 oraz Windows E3**. Umożliwiają one zarządzanie oraz podnoszenie poziomu bezpieczeństwa komputerów, urządzeń mobilnych i aplikacji. Organizacje mogą egzekwować filtrowanie Internetu, aby blokować ryzykowne witryny (w tym nieautoryzowane narzędzia AI) oraz aktualizować urządzenia za pomocą poprawek zabezpieczeń za pośrednictwem funkcji **Autopoprawka Windows i Autopilot**. Te mechanizmy kontroli pomagają utrzymać urządzenia w dobrej kondycji, zarządzać nimi oraz zapewniać aktualność poprawek zabezpieczeń, zmniejszając obszar podatny na ataki. Ujednolicone zarządzanie urządzeniami klienckimi i zarządzanie urządzeniami pozwala organizacjom zabezpieczać urządzenia służbowe oraz zapewniać zgodność aplikacji, niezależnie od tego, czy pracownicy korzystają z urządzeń własnych, czy udostępnionych przez firmę.

Chroń dane, korzystając z funkcji takich jak etykiety poufności i ochrona przed utratą danych.

Pakiet Microsoft 365 E3 zapewnia podstawowe funkcje usługi **Purview** — etykiety poufności, szyfrowanie i ochrona przed utratą danych (DLP) — w celu ochrony informacji wrażliwych w dokumentach i wiadomościach e-mail. Po opublikowaniu zasad etykiet pracownicy mogą klasyfikować pliki zawierające dane finansowe, dane osobowe lub własność intelektualną (na przykład nadając etykietę poufności „Poufne"), stosując szyfrowanie i kontrolę dostępu. Zasady DLP mogą wykrywać i ograniczać nieautoryzowane udostępnianie w usługach **Exchange Online, Microsoft Office SharePoint Online oraz OneDrive dla Firm**. Zabezpieczenia te są stosowane nawet w przypadku korzystania z rozwiązania **Microsoft 365 Copilot**: Copilot przestrzega wymagań etykiety poufności na najwyższym poziomie i zapobiega dostępowi oraz analizie chronionych treści przez użytkowników bez uprawnień.

Uzyskaj wgląd w niezatwierdzone narzędzia AI i podejmuj świadome działania.

Microsoft 365 E3 oferuje usługę **Cloud App Discovery**, która pomaga zrozumieć, jakie aplikacje AI są używane (spośród dostępnych w wykazie aplikacji w chmurze), przez kogo oraz jakie wyniki oceny ryzyka im przypisano, dzięki czemu można określić, jakie działania podjąć na podstawie tych informacji. Jeśli aplikacja zostanie uznana za zbyt ryzykowną, dział IT może użyć rozwiązania **Ochrona punktu końcowego w usłudze Defender P1**, aby ograniczyć możliwości odwiedzania danego adresu URL przez użytkowników na zarządzanych urządzeniach z systemem Windows 11. Jeśli na przykład odkryjesz, że 100 użytkowników korzysta z określonego narzędzia do generowania obrazów AI, które nie zostało sprawdzone ani zatwierdzone przez dział IT — dział IT może to zbadać, opierając się na standardach bezpieczeństwa i zgodności organizacji. Jeśli aplikacja zostanie uznana za ryzykowną, dział IT może zaproponować zatwierdzoną alternatywę. Dzięki tym możliwościom możesz ograniczyć ryzyko związane z nieautoryzowanym użyciem AI i podejmować przemyślane decyzje dotyczące użycia AI, odpowiednie dla Twojej organizacji.

Udostępniaj zatwierdzone aplikacje AI, takie jak Microsoft 365 Copilot.

Udostępnianie zatwierdzonych aplikacji AI zapewnia znaczącą wartość, umożliwiając pracownikom dostęp do zaawansowanych, zatwierdzonych narzędzi spełniających standardy bezpieczeństwa i zgodności Twojej organizacji. Aby na przykład pracownicy nie sięgali po niesprawdzone generatory obrazów AI lub czatboty, dział IT może zaoferować zatwierdzone alternatywy — takie jak **Microsoft 365 Copilot** — monitorowane i wspierane przez obowiązujące zasady firmy oraz zintegrowane z tymi zasadami. **Microsoft 365 Copilot** to bezpieczne, korporacyjne rozwiązanie AI, głęboko zintegrowane z pakietem Microsoft 365. **Copilot** pozwala pracownikom pracować mądrzej, automatyzować rutynowe zadania i generować szczegółowe informacje — a wszystko z poszanowaniem zasad ochrony tożsamości i ochrony danych. Takie podejście ogranicza użycie niezatwierdzonych zasobów IT (shadow IT), pomaga ograniczyć wycieki danych oraz daje organizacjom wgląd w sposoby użycia AI oraz ich kontrolę.

Możliwości te nie działają w izolacji — wzajemnie się wzmacniają, tworząc zintegrowaną, wielowarstwową ochronę. Zasady obsługi tożsamości, urządzeń i ochrony danych współdziałają, aby pomóc łagodzić zagrożenia. Gdy zespoły ds. bezpieczeństwa wiedzą, że istnieją takie środki kontroli, bezpieczeństwo może stać się czynnikiem wspomagającym innowacje, a nie barierą.

Microsoft 365 E3 umożliwia wdrożenie odpowiednich mechanizmów kontrolnych, dzięki którym Twoja organizacja może wprowadzać innowacje z wykorzystaniem AI bez naruszenia zabezpieczeń.

Kontynuuj swoją drogę do wdrożenia AI

Każda organizacja jest na drodze do odkrycia, jak AI może najlepiej służyć jej celom. Obietnica jest kusząca — ale wdrażanie AI musi iść w parze z solidną ochroną. Dzięki pakietowi Microsoft 365 E3 nie trzeba między nimi wybierać. Otrzymujesz potężne rozwiązanie, które podnosi poziom bezpieczeństwa i zgodności, dzięki czemu możesz pewnie korzystać z AI.

Oceń gotowość zabezpieczeń AI.

Microsoft oferuje **ocenę bezpieczeństwa AI**[3]. To internetowe narzędzie do przeprowadzania ocen (dostępne pod adresem security-for-ai-assessment.microsoft.com) przedstawia rekomendacje dotyczące poprawy bezpieczeństwa AI na podstawie udzielonych przez Ciebie informacji. Pomaga ono ocenić aktualny poziom bezpieczeństwa AI w organizacji w oparciu o cztery kluczowe aspekty: **Przygotowanie**, **Odkrywanie**, **Ochrona** oraz **Zarządzanie**, a także przedstawia praktyczne rekomendacje.

Dowiedz się więcej i skontaktuj się z Microsoft.

Jeszcze lepiej poznaj możliwości Microsoft 365 E3 i dowiedz się, jak mogą one pomóc Ci pewnie wdrożyć AI. www.microsoft.com/en-us/microsoft-365/enterprise/e3?activetab=pivot:overviewtab. Możesz również skontaktować się z zespołem ds. kont Microsoft lub partnerem.

1. Work Trend Index Annual Report, 2025: The Year the Frontier Firm Is Born Microsoft, Inc., kwiecień 2025 r. Microsoft przeanalizował dane z ankiet przeprowadzonych wśród 31 000 pełnoetatowych lub samozatrudnionych pracowników umysłowych z 31 krajów (w okresie od 6 lutego 2025 r. do 24 marca 2025 r.), trendów na rynku pracy w serwisie LinkedIn oraz bilionów sygnałów dotyczących produktywności Microsoft 365.
2. Second Annual Generative AI Study: Business Rewards vs. Security Risks, iSMG, Inc., luty 2025 r. — na podstawie ankiety obejmującej ponad 360 profesjonalistów z branży biznesowej i cyberbezpieczeństwa, przeprowadzonej w III kwartale 2024 r.
3. Ocena bezpieczeństwa AI: security-for-ai-assessment.microsoft.com/ Dokładność wyników zależy od dokładności danych wejściowych. Raport ma wyłącznie charakter informacyjny i nie gwarantuje wydajności ani rezultatów. Nie należy interpretować go jako zobowiązania ze strony Microsoft. Rzeczywiste rezultaty mogą się różnić w zależności od czynników, takich jak lokalizacja, sposób zakupu i użytkowanie. Microsoft nie udziela żadnej rękojmi, wyraźnej ani dorozumianej, dotyczącej treści niniejszego raportu lub witryny internetowej.
4. Przedstawione scenariusze są fikcyjne i służą wyłącznie celom ilustracyjnym.