Microsoft 365 Copilot

Zapewnienie bezpieczeństwa danych w erze AI

Przewodnik dla liderów IT

E-book

Ten przewodnik jest skierowany do liderów IT, do których należy wdrażanie AI przy jednoczesnym zapewnieniu bezpieczeństwa danych ich organizacji. Informacje tu zawarte pomogą zrozumieć zagrożenia, jakie sztuczna inteligencja stwarza dla bezpieczeństwa danych i prywatności, zapewniając jednocześnie wgląd niezbędny do sprawnego przeprowadzenia transformacji firmy w kierunku AI.

Spis treści

01

Nowe zasady pracy opartej na AI

Generatywna AI otwiera nowe drzwi dla innowacji. Pomaga zespołom pracować szybciej i inteligentniej niż kiedykolwiek wcześniej. Dla innowacyjnych organizacji AI to nie tylko kolejny trend technologiczny — to imperatyw biznesowy, który ma zasadnicze znaczenie dla ich sposobu działania, dostarczania wartości i utrzymywania przewagi konkurencyjnej.

Jednak to szybkie wdrożenie niesie ze sobą nowe i spotęgowane wyzwania, którym liderzy IT muszą proaktywnie stawić czoła i które muszą kontrolować. Systemy AI mogą aktywnie wyszukiwać i łączyć informacje w całym ekosystemie danych, zwiększając ryzyko w zakresie bezpieczeństwa wykraczające poza tradycyjne narzędzia. Pomimo szybkiego rozwoju AI, tylko **1 proc.** organizacji zgłasza, że w pełni zintegrowało AI ze swoimi przepływami pracy przy zachowaniu odpowiednich protokołów bezpieczeństwa.[1] Wdrażając solidne środki bezpieczeństwa i zarządzania od samego początku korzystania z AI, zespół może skutecznie chronić dane wrażliwe, zachować zgodność z wymogami i zabezpieczyć informacje organizacji, nie blokując przy tym rozwoju innowacji.

Fala wdrażania AI już nadeszła

02

Zrozumienie wpływu AI na bezpieczeństwo danych

Zanim zajmiemy się konkretnymi wyzwaniami, ważne jest, aby zrozumieć, w jaki sposób AI zasadniczo zmienia krajobraz bezpieczeństwa danych. W przeciwieństwie do tradycyjnego oprogramowania, które uzyskuje dostęp do danych tylko po otrzymaniu konkretnych instrukcji, generatywna AI aktywnie przetwarza, analizuje i tworzy treści w oparciu o wszystkie otrzymane informacje.

Różnica ta jest znacząca z kilku powodów:

- Narzędzia AI mogą odkrywać między danymi powiązania, których ludzie mogliby nie zauważyć.
- Mogą automatycznie syntetyzować informacje z wielu źródeł.
- Mogą generować nowe treści, które zawierają elementy danych wrażliwych.

Tradycyjne narzędzia bezpieczeństwa prawdopodobnie nie zostały zaprojektowane z myślą o tych funkcjach. Konwencjonalne oprogramowanie podąża przewidywalnymi ścieżkami podczas uzyskiwania dostępu do danych, natomiast AI może wybierać nieoczekiwane drogi przez ekosystem informacyjny, potencjalnie narażając dane wrażliwe w sposób, który trudno przewidzieć.

Ta fundamentalna zmiana wymaga nowych podejść do bezpieczeństwa i zarządzania danymi, które dotyczą zwłaszcza interakcji AI z zasobami informacyjnymi organizacji.

03

Problem z niezatwierdzonymi narzędziami AI (shadow AI)

Niezależnie od tego, na jakim etapie wdrażania AI się znajdujesz, Twoi pracownicy już znaleźli własne rozwiązania, korzystając z niezatwierdzonych narzędzi AI (shadow AI).

Takie nieautoryzowane użycie tworzy znaczące luki w zabezpieczeniach. Gdy pracownicy udostępniają dane firmowe zewnętrznym systemom AI, omijają istniejące mechanizmy kontroli bezpieczeństwa i tworzą w zabezpieczeniach luki, na które większość organizacji nie jest przygotowana.

Shadow AI to nie tylko kwestia bezpieczeństwa — może to być objaw niezaspokojonych potrzeb w zakresie wydajności w organizacji. Gdy pracownicy sięgają po niezatwierdzone narzędzia, sygnalizują, gdzie oficjalne systemy nie spełniają ich wymagań. Rozwiązanie problemu niezatwierdzonych narzędzi AI (shadow AI) wymaga zarówno lepszego zarządzania, jak i rozwiązań zwiększających wydajność.

Dlaczego pojawia się niezatwierdzona AI:

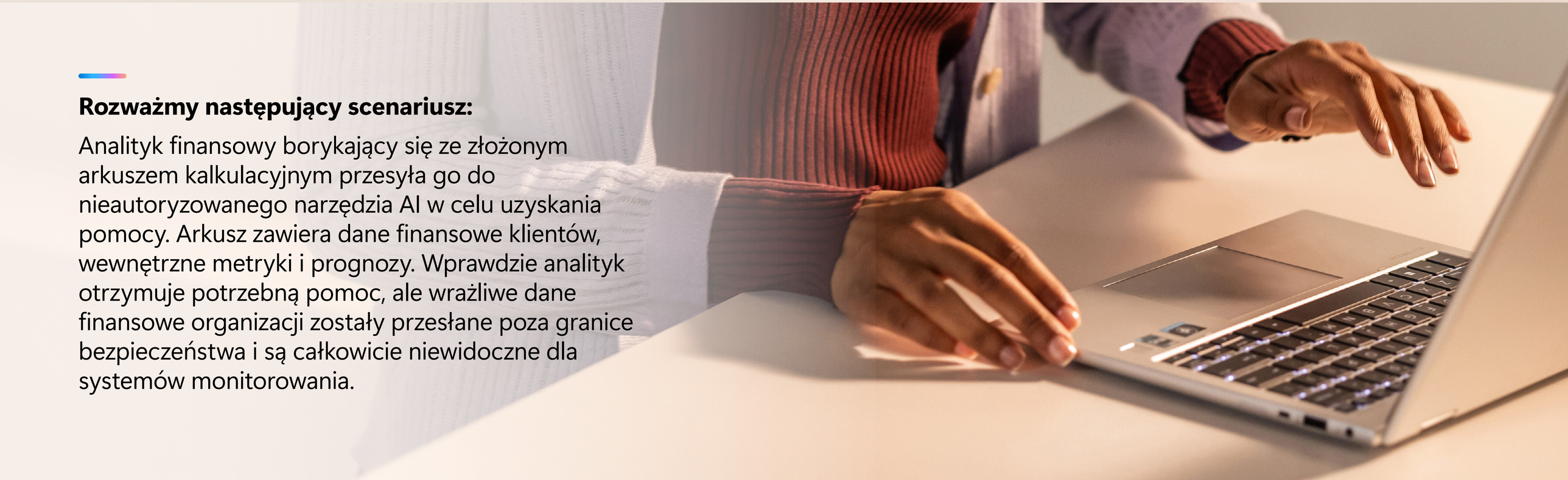
- Pracownicy chętnie zwiększają wydajność dzięki imponującym możliwościom AI.
- Dzienne obciążenia pracą coraz częściej przekraczają dostępny czas i energię.
- Zespoły stają w obliczu rosnącej presji, aby dostarczać więcej przy tych samych zasobach.
- Narzędzia AI dla konsumentów oferują natychmiastowe rozwiązania bez barier zatwierdzania.
- Oficjalne procesy zamówień IT nie mogą dorównać tempu innowacji.

Ryzyko związane z niezatwierdzonymi narzędziami AI:

- Brak dokładnych informacji, jakie dane firmowe są przetwarzane przez zewnętrzne systemy AI.
- Brak gwarancji, że informacje poufne nie są przetrzymywane.
- Brak spójnych standardów bezpieczeństwa na różnych platformach AI.
- Brak możliwości audytu w celu zapewnienia zgodności z przepisami.
- Brak integracji z istniejącą infrastrukturą bezpieczeństwa.

Rozważmy następujący scenariusz:

Analityk finansowy borykający się ze złożonym arkuszem kalkulacyjnym przesyła go do nieautoryzowanego narzędzia AI w celu uzyskania pomocy. Arkusz zawiera dane finansowe klientów, wewnętrzne metryki i prognozy. Wprawdzie analityk otrzymuje potrzebną pomoc, ale wrażliwe dane finansowe organizacji zostały przesłane poza granice bezpieczeństwa i są całkowicie niewidoczne dla systemów monitorowania.



04

Rzeczywistość BYOAI

Bez wyraźnych wskazówek kierownictwa pracownicy coraz częściej samodzielnie wdrażają AI — **78 proc.** użytkowników AI stosuje podejście „przynieś własną AI" (bring your own AI, BYOAI) w pracy.[2] Trend ten jest jeszcze bardziej widoczny w małych i średnich firmach, w których **80 proc.** pracowników stosuje praktyki BYOAI.[2]

Takie niesankcjonowane podejście ma poważne wady. Pracownicy często utrzymują korzystanie z AI w tajemnicy — **52 proc.** niechętnie przyznaje się do używania AI w ważnych zadaniach, a **53 proc.** martwi się, że korzystanie z AI sprawia, że wydają się łatwi do zastąpienia.[2] Ukrywanie tego nie tylko uniemożliwia organizacjom uzyskanie pełnych korzyści ze strategicznego wdrażania AI, ale także stwarza poważne luki w zabezpieczeniach w środowisku, gdzie liderzy uznają cyberbezpieczeństwo i prywatność danych jako swoją **główną** obawę.[2]

Biorąc pod uwagę powszechne użycie i nieunikniony wzrost zastosowań AI, nie chodzi o to, CZY zezwolić na stosowanie AI w organizacji, ale JAK zapewnić bezpieczne rozwiązanie, które zaspokoi potrzeby pracowników, a jednocześnie zapewni bezpieczeństwo danych.

05

Labirynt regulacji prawnych

Ramy prawne dotyczące prywatności i bezpieczeństwa danych stanowią kolejną warstwę złożoności przy wdrażaniu AI. Wprawdzie niektóre struktury zostały specjalnie zaprojektowane do zarządzania AI, jednak inne mają szersze zastosowania, które nadal wpływają na postępowanie z informacjami—a kary za naruszenia są surowe.

Gdy pracownicy korzystają z narzędzi AI bez odpowiedniego nadzoru, mogą przypadkowo spowodować naruszenie zgodności z przepisami. Sztuczna inteligencja zwiększa to ryzyko, ponieważ może uzyskiwać dostęp do informacji regulowanych, łączyć je i ujawniać w sposób, w jaki tradycyjne technologie tego nie potrafią.

Najważniejsze regulacje dotyczące wykorzystania AI:

RODO

Ogólne rozporządzenie o ochronie danych osobowych w Unii Europejskiej daje obywatelom kontrolę nad ich danymi osobowymi i wymaga wyraźnej zgody na ich przetwarzanie.

Unijna ustawa o AI

Kompleksowa struktura Unii Europejskiej zaprojektowana specjalnie pod kątem regulacji systemów AI w oparciu o poziomy ryzyka.

HIPAA

To amerykańskie prawo federalne dotyczące opieki zdrowotnej ustanawia surowe standardy postępowania z chronionymi informacjami dotyczącymi stanu zdrowia.

Ramy zarządzania ryzykiem związanym z AI opracowane przez NIST

Te nieobowiązkowe amerykańskie wytyczne pomagają organizacjom radzić sobie z ryzykiem podczas projektowania, opracowywania i wdrażania systemów AI.

Zagrożenia dla zgodności z przepisami związane z AI:

- Dane klienta są przetwarzane na serwerach poza zatwierdzonymi regionami.
- Dane osobowe są wykorzystywane bez odpowiedniej zgody.
- Dane wrażliwe są przechowywane w systemach bez odpowiedniej kontroli.
- Brak ścieżki audytu dotyczącej sposobu dostępu do chronionych informacji i ich wykorzystywania.
- Treści generowane przez AI, które naruszają specyficzne dla danego sektora wymagania zgodności z przepisami.

Naruszenia te mogą prowadzić do poważnych konsekwencji:

- Wysokie kary finansowe (grzywny w ramach RODO mogą wynosić **4 proc.** globalnych przychodów).[4]
- Wymogi dotyczące powiadamiania zainteresowanych stron o naruszeniach danych.
- Działania prawne osób, których to dotyczy.
- Nadszarpnięcie reputacji firmy i zaufania klientów.

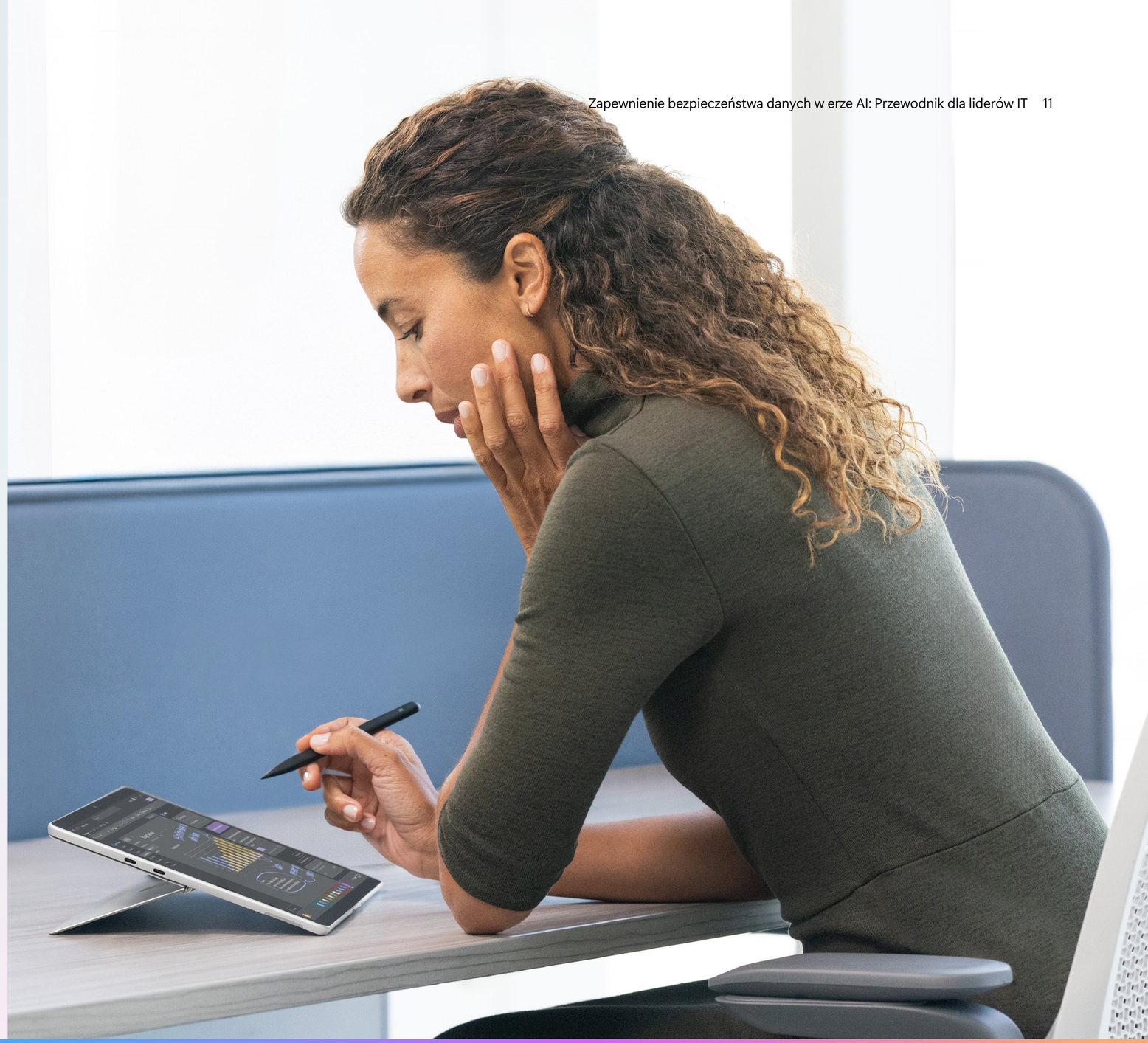
W miarę wzrostu wykorzystania sztucznej inteligencji w całej organizacji potrzebne jest zarządzanie, które pomoże pracownikom pracować wydajnie, a jednocześnie zachować zgodność organizacji z przepisami mającymi wpływ na firmę i klientów.

06

Struktura zapewniająca bezpieczeństwo zmieniających się rozwiązań AI

Biorąc pod uwagę, że niezatwierdzone narzędzia AI (shadow AI), korzystanie z własnych narzędzi AI (BYOAI) i przepisy stwarzają znaczące ryzyko, potrzebne jest usystematyzowane podejście do oceny rozwiązań AI, które umożliwi organizacji wprowadzanie innowacji przy jednoczesnej ochronie danych wrażliwych i zapewnieniu zgodności ze zmieniającymi się przepisami.

Poniższe zestawienie zawiera sześć prostych pytań pozwalających ocenić, czy platforma AI spełnia wszystkie oczekiwania.



Pytanie 1

Czy od samego początku oferuje zabezpieczenia klasy korporacyjnej?

W odpowiednim rozwiązaniu dbałość o bezpieczeństwo nie polega na reagowaniu na problemy po ich wystąpieniu, ale zmienia się w proaktywne wyszukiwanie luk w danych organizacji zanim staną się one poważniejszymi problemami.

Poszukaj rozwiązań, które:

- Zapewniają widoczność całego ekosystemu danych w czasie rzeczywistym.
- Automatycznie identyfikują potencjalne zagrożenia związane z danymi, zanim te staną się incydentami.
- Chronią informacje wrażliwe na każdym poziomie.

Pytanie 2

Czy można łatwo zaadoptować i ulepszyć istniejące zabezpieczenia?

Zasady bezpieczeństwa organizacji powinny bezproblemowo współpracować z AI. Dostawca rozwiązań AI powinien respektować istniejące ramy bezpieczeństwa i integrować się z nimi, a nie wymagać tworzenia zupełnie nowych.

Poszukaj rozwiązań, które:

- Bezproblemowo wdrażają istniejące zasady bezpieczeństwa, etykiety wrażliwości i ustawienia ochrony informacji.
- Stosują szczegółową kontrolę dostępu na poziomie indywidualnym, aby żaden użytkownik nie miał dostępu do danych, do których nie powinien go mieć.
- Aktywnie oznaczają próby obejścia kontroli dostępu.

Pytanie 3

Czy zawiera wbudowane mechanizmy zarządzania i kontroli prywatności?

Ponieważ narzędzia AI działają bardziej proaktywnie, środki bezpieczeństwa również muszą być proaktywne. Wdrożenie silnego zarządzania danymi ustala wyraźne granice, w których pracownicy mogą bezpiecznie wprowadzać innowacje bez narażania na ryzyko informacji wrażliwych.

Poszukaj rozwiązań, które:

- Centralizują zarządzanie AI dzięki automatycznemu egzekwowaniu zasad we wszystkich działaniach.
- Mają wbudowane funkcje wczesnego wykrywania potencjalnego nadmiernego udostępniania danych.
- Są zgodne z obowiązującymi przepisami i gwarantują taką zgodność z przepisami dotyczącymi wykorzystania AI.

Pytanie 4

Czy można je wdrażać spójnie w całej organizacji?

Każdy pracownik ma własny styl pracy, własny harmonogram i może przebywać w dowolnym zakątku świata. Sztuczna inteligencja powinna przynieść korzyści wszystkim.

Poszukaj rozwiązań, które:

- Zapewniają bezproblemowe konfigurowanie i łatwe wdrażanie AI w codziennych przepływach pracy.
- Zapewniają elastyczny dostęp, od darmowego czatu AI po skalowalne rozwiązania wykorzystujące agenty.
- Pomagają pracownikom korzystać z AI i włączać ją do swojej pracy.

Pytanie 5

Czy płynnie integrują się z istniejącymi strukturami?

Twoja firma działa obecnie w oparciu o własną cyfrową infrastrukturę programów, aplikacji i nie tylko.

Poszukaj rozwiązań, które:

- Bezproblemowo integrują się z narzędziami i programami, aby zminimalizować zakłócenia.
- Zapewniają nieprzerwaną obsługę AI we wszystkich aplikacjach, dzięki czemu praca może płynnie przepływać między różnymi narzędziami.
- Automatyzują i optymalizują zadania w ramach istniejących przepływów pracy.

Pytanie 6

Czy użytkownicy mogą wprowadzać innowacje?

Zasadniczo sztuczna inteligencja powinna zmienić sposób wykonywania pracy. Nie chodzi tu tylko o automatyzację, ale także o zwiększenie produktywności i wspieranie innowacji.

Poszukaj rozwiązań, które:

- Przekształcają czasochłonne czynności w usprawnione procesy.
- Automatyzują powtarzalne zadania.
- Umożliwiają pracownikom zaoszczędzenie czasu i skupienie się na najważniejszych zadaniach.

07

Microsoft 365 Copilot: AI godna zaufania

Microsoft 365 Copilot to rozwiązanie generatywnej AI, które powstało w celu zapewnienia solidnych zabezpieczeń, zarządzania i kontroli dostępu — gwarantując jednocześnie bezpieczne wdrażanie i ciągłe innowacje. Zwiększa produktywność dzięki intuicyjnym narzędziom, takim jak czat Copilot, który działa tam, gdzie Ty, oraz Copilot Studio, w którym Twój zespół może tworzyć niestandardowe agenty AI bez umiejętności programowania.

Copilot bezproblemowo integruje się ze środowiskiem Microsoft 365, dziedzicząc uprawnienia użytkownika, etykiety poufności, zasady zapobiegania utracie danych i wymagania dotyczące geograficznego przechowywania danych — bez dodatkowego konfigurowania. Wdrażając AI w narzędziach, z których pracownicy już korzystają, Copilot zmniejsza ryzyko dla bezpieczeństwa, jednocześnie przechowując dane w zaufanym środowisku Microsoft 365.

Zobowiązania Microsoft gwarantują, że są one przez cały czas kontrolowane przez organizację:

- Dane są bezpieczne w spoczynku i podczas przesyłania.
- Twoje dane nie są wykorzystywane do trenowania modeli AI.
- Ty decydujesz, jakie informacje trafiają do chmury.
- Ochrona przed zagrożeniami związanymi z bezpieczeństwem AI i prawami autorskimi.

Specjalnie zaprojektowane narzędzia do zarządzania, takie jak Copilot Control System i SharePoint Advanced Management, zapewniają zespołom IT wgląd w dane, kontrole i dzienniki audytu potrzebne do utrzymania zgodności.

Dzięki usłudze Microsoft 365 Copilot nie musisz wybierać między innowacyjnością a bezpieczeństwem — możesz mieć i to i to.

08

Bezpieczna droga do transformacji AI

Rewolucja w zakresie AI to dla liderów IT wyjątkowa okazja do zapewnienia strategicznej wartości poprzez zrównoważenie innowacji i bezpieczeństwa.

Wdrażając bezpieczne narzędzia AI, takie jak Microsoft 365 Copilot, zapewnisz pracownikom narzędzia zwiększające produktywność, a jednocześnie wyeliminujesz ryzyko korzystania z niezatwierdzonych narzędzi AI (shadow AI). Rozwój polega na bezpiecznym wprowadzaniu innowacji. Twoje przywództwo w zakresie bezpiecznego wdrażania AI sprawi, że IT stanie się narzędziem umożliwiającym transformację, pomagając organizacji rozwijać się w nowej erze, jednocześnie zapewniając bezpieczeństwo i zgodność danych.

Rozpocznij korzystanie z usługi Microsoft 365 Copilot

Źródła:

[1] „Superagency in the workplace: Empowering people to unlock AI's full potential", McKinsey & Company, 28 stycznia, 2025 r. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work.

[2] „AI wspomagająca pracę już tu jest. A wraz z nią nowe wyzwania". Indeks trendów w pracy, Microsoft, 8 maja 2024 r. https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part.

[3] „Czy AI naprawi środowisko pracy?", „Trendy na rynku pracy", 9 maja 2023 r. Microsoft. https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work.

[4] „Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)", Parlament Europejski i Rada Unii Europejskiej, 27 kwietnia 2016 r. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.