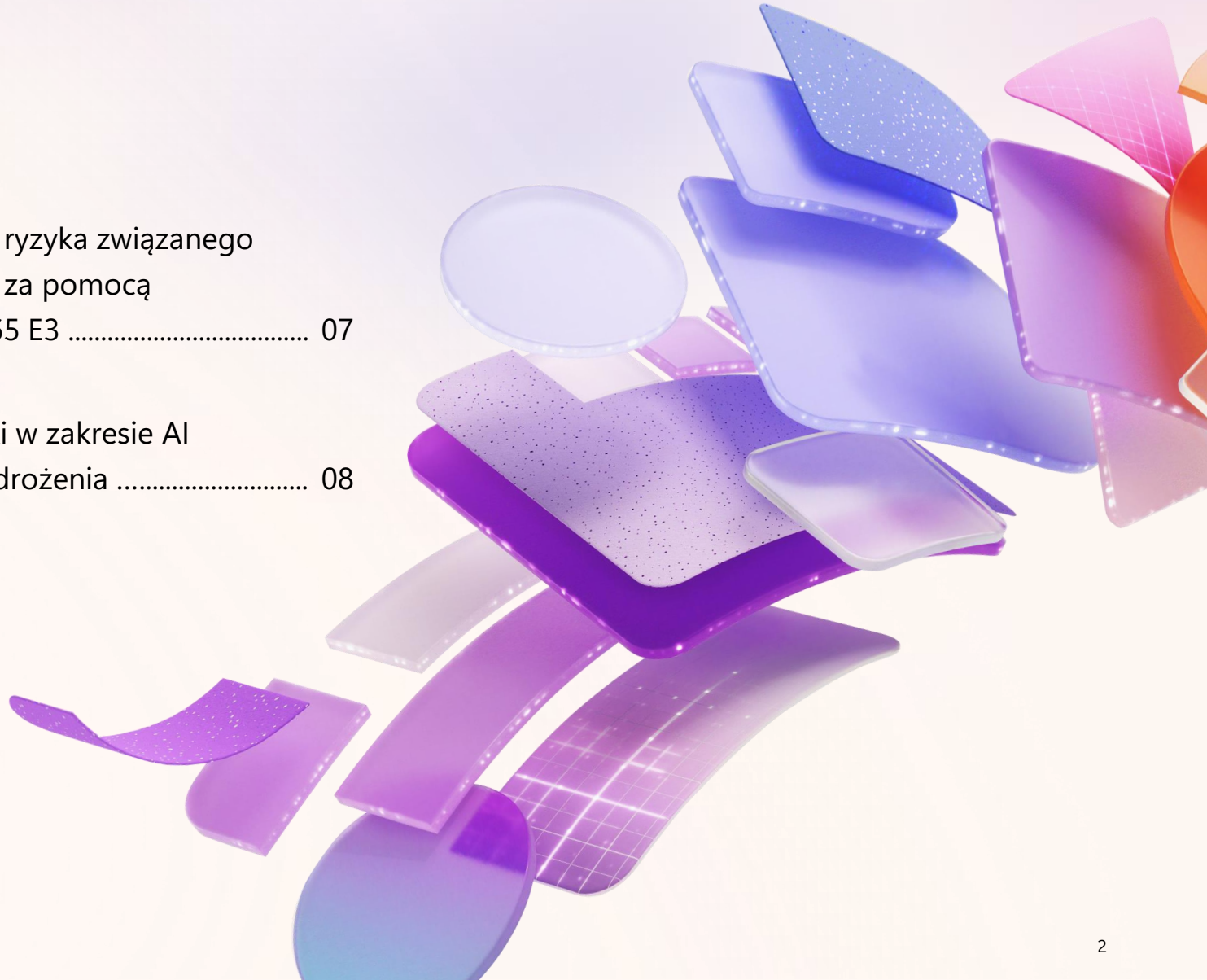
Microsoft 365

Od nadzoru do spostrzeżeń: zarządzanie ryzykiem związanym z shadow AI

Spis treści



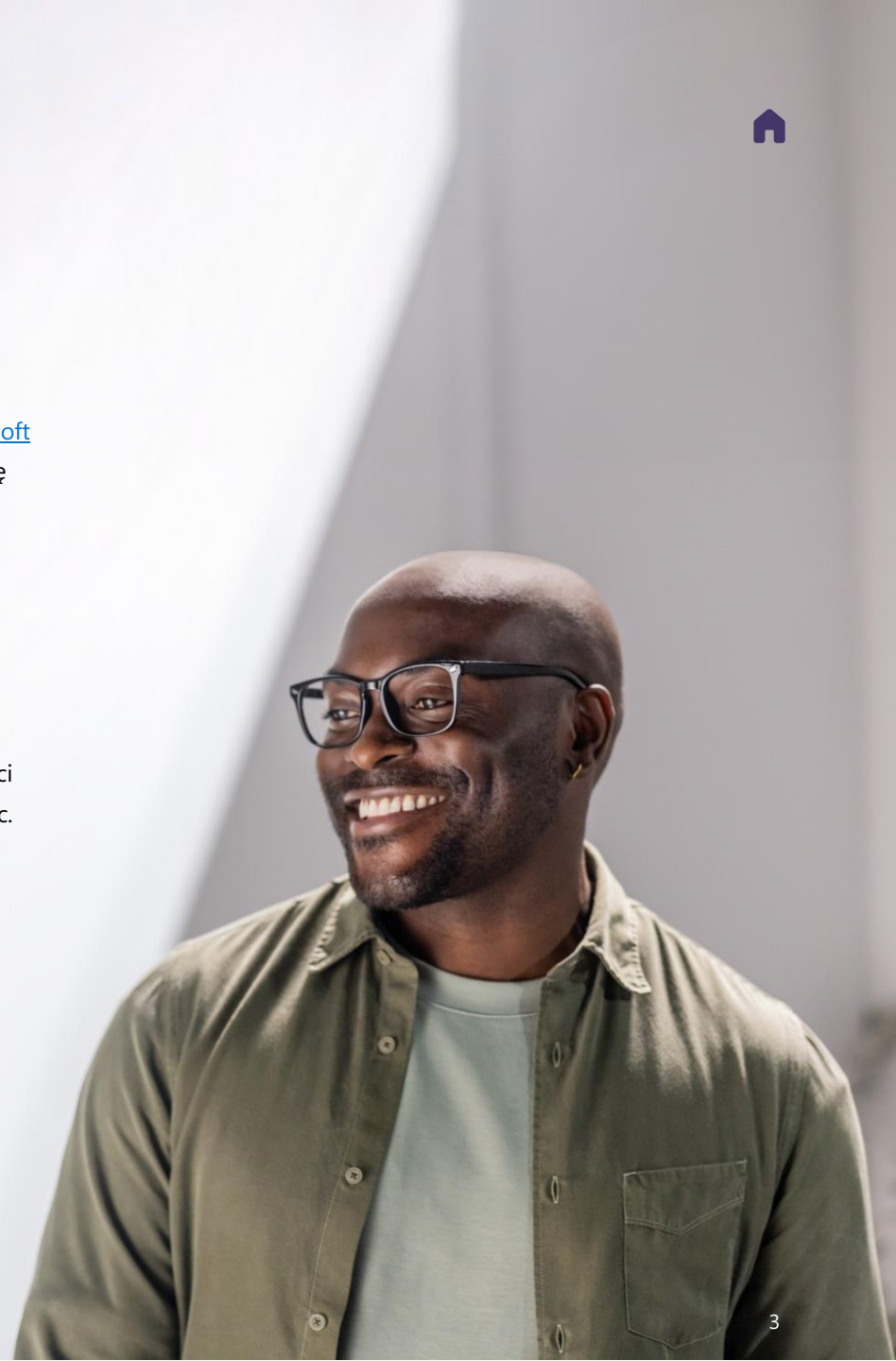
Wprowadzenie

W najnowszym raporcie o trendach na rynku pracy ponad 80 proc. pracowników umysłowych ankietowanych w 31 krajach — w tym pracownicy i liderzy — stwierdziło, że odczuwa brak czasu lub energii na wykonywanie swojej pracy. Ponadto ponad 50 proc. ankietowanych liderów biznesowych uważa, że aby osiągnąć cele, konieczne jest zwiększenie produktywności[1]. Według raportu Microsoft Work Trend Index z 2024 r. wielu pracowników poszukuje narzędzi generatywnej AI, aby wypełnić tę lukę i nie czeka na oficjalną zgodę działu IT, zanim zacznie z nich korzystać.

Gdy narzędzia funkcjonują poza nadzorem IT, mogą stanowić dla organizacji zagrożenie w zakresie bezpieczeństwa i zgodności z przepisami. Shadow AI — czyli wykorzystywanie narzędzi AI niezatwierdzonych przez dział IT — wyłania się jako najnowsza forma wykorzystywania niezatwierdzonych zasobów IT (shadow IT) we współczesnych miejscach pracy.

W miarę jak wdrażanie AI przyspiesza, liderzy biznesowi starają się być na bieżąco i łagodzić potencjalne ryzyka, które mogą stwarzać te narzędzia. W niedawnym 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] Ponad 90 proc. ankietowanych dyrektorów ds. informatyki (CIO) i dyrektorów ds. technologii (CTO) zgłosiło, że generatywna AI już doprowadziła lub doprowadzi do większych inwestycji w cyberbezpieczeństwo w ich organizacjach.[3]

W tym e-booku poznasz typowe scenariusze wykorzystania niezatwierdzonych zasobów AI (shadow AI), zrozumiesz potencjalne zagrożenia dla organizacji, poznasz pięć sposobów zarządzania nimi oraz zobaczysz, jak Microsoft 365 E3 może w tym pomóc.



[1] **Trendy na rynku pracy: raport roczny (2025 r.), Microsoft Inc., kwiecień 2025 r.** Microsoft przeanalizował dane z ankiet przeprowadzonych wśród 31 000 pełnoetatowych lub samozatrudnionych pracowników umysłowych z 31 krajów, zebranych w okresie od 6 lutego 2025 r. do 24 marca 2025 r., trendy na rynku pracy LinkedIn oraz biliony sygnałów dotyczących produktywności w ramach usługi Microsoft 365.

[2] **iSMG Second Annual Generative AI Study: Business Rewards vs. Security Risks,** na podstawie odpowiedzi z ankiety od ponad 360 specjalistów ds. biznesu i cyberbezpieczeństwa w trzecim kwartale, z 6 regionów (Ameryka Północna, Europa, Azja, Ameryka Południowa, Australia i Afryka).

[3] **The AI Security Balancing Act: From Risk to Innovation", NTT DATA, czerwiec 2025,** na podstawie danych z ankiety NTT DATA przeprowadzonej wśród ponad 2300 decydentów ds. GenAI na szczeblu kierowniczym, w tym 1500 członków najwyższego kierownictwa, z 34 krajów.

Co to jest shadow AI? Dlaczego widoczność ma znaczenie?

Termin "shadow AI" odnosi się do wykorzystywania przez pracowników narzędzi i aplikacji opartych na AI bez wyraźnej zgody lub nadzoru działów IT, często poza zasięgiem oficjalnych ram bezpieczeństwa i zgodności. Gdy pracownicy szukają sposobów na zwiększenie produktywności i sprostanie rosnącym wymaganiom związanym z obciążeniem pracą, mogą uciekać się do nieautoryzowanych rozwiązań, aby usprawnić zadania, współpracować lub generować nowe treści, często nie zdając sobie sprawy z potencjalnych zagrożeń. Narzędzia shadow AI są niewidoczne dla działu IT, przez co organizacjom trudno jest stwierdzić, jakie aplikacje są używane i które z nich stanowią największe ryzyko.

Dlaczego widoczność shadow AI jest tak ważna

Gdy dział IT nie zna aplikacji lub usługi, nie może jej zabezpieczyć ani wspierać. Ta *luka w widoczności* utrudnia dokładną identyfikację, zarządzanie i łagodzenie potencjalnych zagrożeń związanych z narażeniem danych wrażliwych, niezgodnością z przepisami oraz utratą kontroli nad informacjami zastrzeżonymi. Liderzy IT i biznesu muszą się dowiedzieć, jakie zasoby shadow AI są wykorzystywane w ich organizacji, zająć się pojawiającymi się zagrożeniami związanymi z wykorzystaniem AI i zdecydować, które narzędzia powinny być dozwolone — z odpowiednimi zabezpieczeniami. Dzięki temu w organizacji pojawi się szansa, aby przekształcić shadow AI z ryzyka w okazję do wdrażania innowacyjnych i bezpiecznych sposobów pracy. Aby to osiągnąć, konieczne jest lepsze wyważenie — umożliwienie pracownikom korzystania z przydatnych narzędzi AI w ramach zarządzanych, bezpiecznych ram w celu ograniczenia potencjalnych zagrożeń.

ANALIZA

Nie można się zabezpieczyć przed zagrożeniami, których nie widać. Jeśli dział IT nie ma wiedzy o używanej aplikacji lub usłudze, nie może jej zabezpieczyć. To jest sedno problemu związanego z Shadow AI, które pokazuje, dlaczego potrzebne jest nowe podejście. Proste zakazanie korzystania ze wszystkich zewnętrznych narzędzi nie będzie praktyczne, jeśli pracownicy uważają, że narzędzia AI są niezbędne do osiągnięcia ich celów. Zamiast tego organizacje muszą wydobyć shadow AI na światło dzienne — dowiedzieć się, z jakich narzędzi korzystają pracownicy, wdrożyć odpowiednie środki kontroli oraz zaoferować bezpieczne, zatwierdzone alternatywy, które odpowiadają potrzebom organizacji. Krótko mówiąc, wyzwaniem jest wyposażenie zespołów w sztuczną inteligencję *bez* narażania bezpieczeństwa.

Shadow AI w miejscu pracy: Przykładowe scenariusze i potencjalne zagrożenia

Shadow AI powstaje w wyniku działań pracowników, którzy chcą zwiększyć swoją produktywność i skuteczność lub wypróbować nową technologię. Poniżej przedstawiono kilka fikcyjnych przykładów ilustrujących, w jaki sposób mogą być wykorzystywane nieautoryzowane narzędzia AI oraz jakie potencjalne zagrożenia mogą stwarzać:

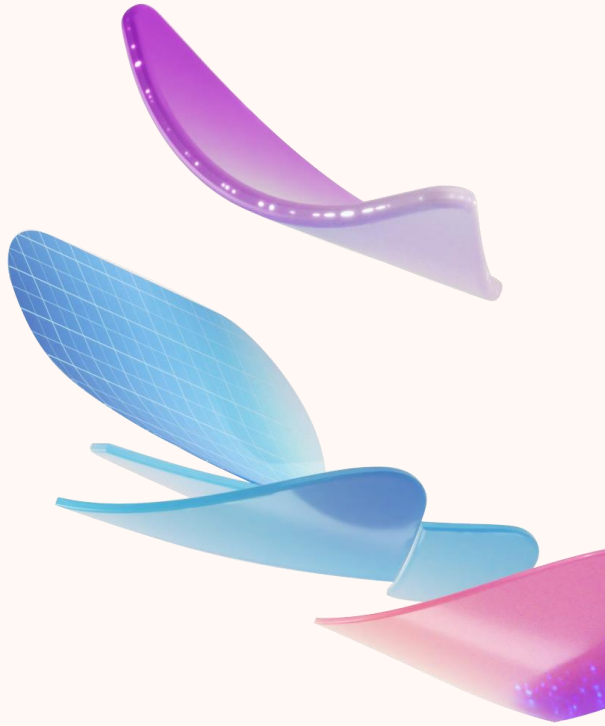
Stanowisko	Przykładowy scenariusz	Potencjalne ryzyko związane z nieautoryzowanymi narzędziami
Marketing	Tworzenie tekstów marketingowych lub projektów przy użyciu narzędzi generatywnej AI i informacji o marce firmy.	Wyciek poufnych informacji o marce lub produkcie; utrata kontroli nad tym, w jaki sposób zewnętrzna usługa AI może przechowywać lub wykorzystywać kreatywne zasoby firmy.
Dział finansowy	Przesyłanie danych finansowych firmy do usługi analitycznej lub wizualizacyjnej opartej na AI w celu uzyskania szybkich wniosków.	Ujawnienie poufnych danych finansowych (budżetów, prognoz) podmiotom zewnętrznym; potencjalne naruszenie zgodności z przepisami (np. RODO), jeśli dane klientów lub pracowników zostaną uwzględnione bez odpowiednich środków ochrony.
Obsługa klienta	Przekazywanie danych klientów lub zapisów czatów wsparcia do narzędzia AI w celu tworzenia odpowiedzi lub podsumowywania spraw.	Naruszenie zasad prywatności i przechowywania danych — poufne informacje o klientach mogą być przechowywane poza systemami firmy; dostawca AI nie udziela gwarancji co do przechowywania danych ani prawidłowego usuwania danych.
Pracownicy pierwszego kontaktu — handel detaliczny	Kierownicy sklepów korzystają z aplikacji do planowania grafików opartych na AI na swoich telefonach, aby optymalizować harmonogramy pracy pracowników.	Dane dotyczące pracowników firmy (imiona i nazwiska, harmonogramy) są przesyłane do niezaakceptowanej oficjalnie aplikacji, co może spowodować problemy z prywatnością. Jeśli sugestie AI nie będą zgodne z przepisami prawa pracy, może dojść do sprzecznych harmonogramów lub naruszeń zasad.
Pracownicy pierwszego kontaktu — opieka zdrowotna	Pielęgniarki lub lekarze korzystają z czatbota opartego na AI, aby pomagać sobie w sporządzaniu notatek z opieki nad pacjentem lub odpowiadać na pytania medyczne.	Informacje o stanie zdrowia pacjenta (PHI) mogą zostać udostępnione zewnętrznym usługom bez żadnych zabezpieczeń, co stanowi naruszenie wymogów zgodności i poufności. Porady medyczne udzielane przez AI mogą być także niezweryfikowane, co stanowi zagrożenie dla bezpieczeństwa.

W każdym z powyższych przypadków indywidualny pracownik miał dobre intencje i szukał sposobu na zwiększenie produktywności, ale w rezultacie mógł narazić organizację na ryzyko.

Informacje firmowe mogą zostać rozproszone na nieautoryzowanych platformach, tworząc *wyzwania związane z zarządzaniem danymi*. Niesprawdzone aplikacje mogą wprowadzać złośliwe oprogramowanie lub powodować luki w zabezpieczeniach, rozszerzając obszar podatny na ataki poza kontrolę działu IT. Mogą również wystąpić konsekwencje związane ze zgodnością z regulacjami. Z punktu widzenia wsparcia IT, jeśli coś pójdzie nie tak z narzędziem shadow AI, pomoc techniczna może nie być w stanie wesprzeć użytkowników końcowych, ponieważ nie ma dostępu do informacji o narzędziu ani kontroli nad nim.

Pięć sposobów zarządzania ryzykiem związanym z shadow AI

Dzięki odpowiedniej strategii i narzędziom można przekształcić shadow AI z potencjalnego zagrożenia w szansę na rozwój kultury bezpiecznych innowacji. Wyposaż zespoły w narzędzia zwiększające produktywność oparte na AI *jednocześnie* zachowując nadzór niezbędny do ochrony firmy. To przejście od mówienia „nie, nigdy" do mówienia „tak — ale z odpowiednimi zabezpieczeniami". Poniższe pięć wskazówek pomoże Ci zarządzać shadow AI w organizacji i przejąć nad nią kontrolę:



01 Odkryj ślad shadow AI, aby ocenić ryzyko i ustalić priorytety

Nie można się zabezpieczyć przed zagrożeniami, których nie widać. Zbierz informacje o aplikacjach używanych w organizacji dzięki dziennikom aktywności. Gdy już wiesz, jakie aplikacje są używane, możesz zidentyfikować odpowiednie narzędzia do obsługi danych wrażliwych, zwracając uwagę na te, które nie są zgodne z zasadami bezpieczeństwa i zasadami zgodności. Dzięki tym informacjom możesz podjąć bardziej przemyślane decyzje, na które aplikacje chcesz zezwolić, monitorować lub ograniczyć, aby ograniczyć potencjalne ryzyko.

02 Wdrażaj szybkie korzyści dzięki politykom bezpieczeństwa i zgodności

Włącz lub zastosuj aktualizacje zasad, aby skuteczniej ograniczyć potencjalne ryzyko związane z wykorzystaniem shadow AI. Możesz stosować zasady dostępu warunkowego, aby ograniczyć użycie aplikacji wysokiego ryzyka, wdrażać polityki ochrony przed utratą danych dla informacji wrażliwych, aby ograniczyć nadmierne udostępnianie i wyciek danych oraz wymuszać podstawowe uwierzytelnianie wieloskładnikowe i zgodność urządzeń dla wszystkich użytkowników. Te kroki pozwalają szybko ograniczyć najbardziej rażące zagrożenia, nawet jeśli nie masz jeszcze pełnych informacji o wykorzystywaniu aplikacji AI.

03 Przeszkol pracowników w zakresie potencjalnych zagrożeń związanych z shadow AI

Często pracownicy nie są świadomi zagrożeń, jakie niesie używanie nieautoryzowanych narzędzi AI w organizacji. Informuj użytkowników o ryzyku związanym z shadow AI, często stosując dobrze umieszczone ostrzeżenia dotyczące ochrony przed utratą danych, przypomnienia o zasadach obowiązujących w firmie oraz krótkie szkolenia, które pomogą skierować użytkowników na bezpieczniejsze praktyki bez konieczności drastycznego egzekwowania przepisów.

04 Zapewnij zatwierdzone narzędzia AI, aby jeszcze bardziej ograniczyć ryzyko

W miarę możliwości oferuj pracownikom zatwierdzone narzędzia AI jako alternatywę dla nieautoryzowanych rozwiązań. Świetnym sposobem na ograniczenie shadow AI jest wdrożenie zatwierdzonego rozwiązania do najczęstszych przypadków użycia w organizacji. Dzięki temu dział IT zachowuje przejrzystość i kontrolę, jednocześnie zapewniając wsparcie użytkownikom w przypadku pojawiających się problemów.

05 Ustanów ciągłe zarządzanie

Zaimplementuj mechanizmy kontroli w rutynowych procesach zarządzania IT — systematycznie analizuj dzienniki aktywności i raporty, aktualizuj polityki wraz z pojawianiem się nowych usług AI oraz informuj kierownictwo o postępach (np. o spadku nieautoryzowanego użycia aplikacji lub zapobieganiu incydentom). Pomoże Ci to zminimalizować potencjalne ryzyka teraz i w przyszłości, w miarę jak ewoluuje otoczenie technologiczne.

Podejmując powyższe kroki, możesz wzmocnić zarówno innowacyjność, jak i bezpieczeństwo.

Pracownicy mogą korzystać z zatwierdzonych rozwiązań AI, a dział IT zachowuje kontrolę i zgodność nad tymi narzędziami.

Wykrywanie ryzyka związanego z shadow AI za pomocą Microsoft 365 E3

Microsoft 365 E3 zapewnia organizacjom możliwości wykrywania niezatwierdzonych zasobów IT, oceny potencjalnych zagrożeń oraz wdrażania zasad bezpieczeństwa i zgodności *bez* hamowania innowacyjności. Ten pakiet zintegrowanych rozwiązań z zakresu produktywności, bezpieczeństwa i zarządzania może umożliwić bezpośrednie stawienie czoła wyzwaniom związanym z shadow AI.

Rozwiązanie Microsoft 365 E3	Jak pomaga zarządzać potencjalnymi zagrożeniami związanymi z AI
Cloud App Discovery	**Wykrywaj niezatwierdzone aplikacje i podejmuj wobec nich działania.** Cloud App Discovery umożliwia przesyłanie dzienników aktywności i tworzenie raportów migawek, co pozwala uzyskać wgląd w ponad 31 000 aplikacji chmurowych — w tym ponad 400 aplikacji generatywnej AI. Pozwala zobaczyć, jakie aplikacje są używane w organizacji, przez kogo i jak często. Te informacje umożliwiają podejmowanie przemyślanych decyzji dotyczących tego, które aplikacje należy dopuścić do użytku, a które ograniczyć.
Ochrona przed utratą danych w Microsoft Purview (DLP)	**Ogranicz wycieki danych wrażliwych.** Microsoft Purview DLP umożliwia definiowanie i stosowanie zasad, które wykrywają informacje wrażliwe oraz blokują lub ograniczają udostępnianie ich w usługach Microsoft 365 dla wiadomości e-mail i plików. Na przykład możesz ustawić regułę monitorującą, audytującą lub blokującą udostępnianie przez użytkowników informacji wrażliwych za pomocą poczty e-mail lub udostępniania plików oraz powiadamiającą użytkownika.
Microsoft Entra ID P1	**Zarządzaj dostępem do aplikacji w chmurze.** Microsoft Entra P1 umożliwia stosowanie zasad dostępu warunkowego w celu kontrolowania, kto może uzyskiwać dostęp do poszczególnych aplikacji i na jakich warunkach. Na przykład możesz zdecydować się wymagać uwierzytelniania wieloskładnikowego lub nawet ograniczyć logowanie się przy użyciu firmowych danych uwierzytelniających do aplikacji o podwyższonym ryzyku. Microsoft Entra P1 umożliwia dostęp do zasobów w chmurze odpowiednim osobom, na zgodnych urządzeniach, na zatwierdzonych warunkach — jednocześnie ograniczając dostęp do niezatwierdzonych aplikacji.
Microsoft Intune P1	**Egzekwuj zasady użytkowania urządzeń i aplikacji.** Microsoft Intune P1 umożliwia zezwolenie na używanie zarządzanych, zgodnych z polityką firmy urządzeń do pracy oraz zapewnia narzędzia do zarządzania tymi urządzeniami. Na przykład może zakazać instalacji niezatwierdzonego oprogramowania na firmowych komputerach PC lub wprowadzić konfiguracje ograniczające dostęp do określonych stron internetowych lub usług.
Ochrona punktu końcowego w usłudze Microsoft Defender P1	**Ogranicz ruch do niezatwierdzonych adresów URL.** Ochrona punktu końcowego w usłudze Microsoft Defender P1 pozwala ograniczyć ryzyko związane z witrynami uznawanymi za niebezpieczne, blokując ruch do niezatwierdzonych adresów URL z urządzeń zarządzanych. Na przykład pracownicy próbujący odwiedzić znaną, ryzykowną witrynę AI na firmowym laptopie zostaną zablokowani przed uzyskaniem do niej dostępu.

Kolejne kroki w zakresie AI Droga do wdrożenia

Wszystko zaczyna się od świadomości, odpowiednich narzędzi i proaktywnego planu. Microsoft 365 E3 zapewnia narzędzia, które umożliwiają organizacjom zbudowanie solidnych fundamentów bezpieczeństwa oraz ram zarządzania dla rozwiązań AI. Uzyskasz wgląd w niezatwierdzone narzędzia, wdrożysz zasady ochrony danych wrażliwych oraz zachowasz kontrolę zarówno nad dostępem użytkowników, jak i zabezpieczeniami urządzenia. Przygotuj się na przejście z reaktywnego podejścia (wyszukiwania i blokowania shadow AI po jej pojawieniu się) do bardziej proaktywnego podejścia, polegającego na kierowaniu wykorzystania AI do bezpiecznych, zarządzanych kanałów. Wykorzystaj ocenę bezpieczeństwa AI i dowiedz się, jak możesz poprawić stan zabezpieczeń dla AI. Dowiedz się więcej o funkcjach dostępnych w Microsoft 365 for Enterprise.