Microsoft Security

Wskaźnik bezpieczeństwa danych

Ujednolicenie ochrony danych i innowacji w zakresie AI

Raport z 2026 r.

Przedmowa

W ostatnim roku organizacje wzmacniały fundamenty, aby stosować mechanizmy kontroli bezpieczeństwa danych i zarządzania w nowych aplikacjach i agentach AI. Rosnąca rola generatywnej AI (GenAI) odmienia dotychczasowy sposób pracy. Według wskaźnika trendów na rynku pracy w 2025 r. większość ankietowanych globalnych pracowników wiedzy deklaruje korzystanie z AI, a ponad 70 proc. z nich przynosi do pracy własne narzędzia AI[1] — co podkreśla rosnący trend w zakresie wdrażania AI. Ale razem z tym pojawiła się nowa pilna potrzeba: widoczność, zarządzanie i ochrona danych są obecnie niezbędnymi warunkami wstępnymi dla bezpiecznych i odpowiedzialnych innowacji.

W trzeciej edycji Wskaźnika bezpieczeństwa danych przyglądamy się temu, jak generatywna AI przekształca podejście do bezpieczeństwa danych. Liderzy ds. bezpieczeństwa potrzebują zintegrowanego widoku swoich danych, aby odpowiedzialnie wdrażać AI. W odpowiedzi na to organizacje odchodzą od rozproszonych narzędzi na rzecz zintegrowanych platform, które zapewniają ciągłą widoczność i spójną ochronę — sprawiając, że bezpieczeństwo i innowacyjność stają się nierozłączne. Aby bezpiecznie wdrożyć AI, organizacje muszą najpierw uzyskać jednolite zrozumienie swoich danych: gdzie się znajdują, kto ma do nich dostęp i w jaki sposób są chronione. Rozdrobnione narzędzia i odizolowane kontrole ustępują miejsca zintegrowanym platformom zapewniającym ciągłą widoczność i spójną ochronę w różnych środowiskach.

W Microsoft wierzymy, że widoczność, operatywność i integracja są kluczem do wykorzystania pełnego potencjału AI, co umożliwia ujednolicona strategia bezpieczeństwa danych. Zintegrowane rozwiązania, które łączą funkcje widoczności, ochrony, wykrywania i badania, umożliwiają bezpieczne skalowanie przy jednoczesnej minimalizacji złożoności. Wspiera to wykrywanie i ograniczanie ryzyka związanego z danymi, a także umożliwia organizacjom odpowiedzialne wykorzystanie AI i przyspieszenie innowacji.

Spostrzeżenia przedstawione w niniejszym dokumencie podkreślają wyraźną prawdę: organizacje najlepiej przygotowane na przyszłość to te, które inwestują w integrację, inteligencję i odpowiedzialną sztuczną inteligencję. Zasady te stanowią podstawę strategii bezpieczeństwa danych, która chroni dzisiejsze ekosystemy cyfrowe i toruje drogę innowacjom jutra.

Zachęcamy do zapoznania się z tymi spostrzeżeniami i wykorzystania ich do wzmocnienia swojego stanu zabezpieczeń, jednocześnie odpowiedzialnie rozwijając zastosowanie AI. Razem możemy zbudować fundament innowacji oparty na bezpieczeństwie, przekształcając złożoność w przejrzystość i przygotowując grunt pod bardziej elastyczną, godną zaufania przyszłość.

Rudra Mitra
Wiceprezes ds. korporacyjnych
Bezpieczeństwo danych i zgodność z przepisami
Microsoft

1. Microsoft, 2025, Trendy na rynku pracy

Wprowadzenie

We współczesnym, szybko zmieniającym się ekosystemie cyfrowym organizacje muszą odnajdywać się w coraz bardziej złożonym krajobrazie bezpieczeństwa danych, by chronić swoją organizację i wyprzedzać pojawiające się zagrożenia. Zespoły ds. bezpieczeństwa znajdują się pod presją, aby osiągać więcej przy ograniczonych zasobach czasu, personelu i środków, nawet gdy ilość danych, które muszą zabezpieczyć, rośnie wykładniczo. Ponieważ rozdrobnione narzędzia prowadzą do luk w widoczności, zwiększają złożoność i podnoszą ryzyko ujawnienia danych, zespoły koncentrują się na konsolidacji rozwiązań oraz wzmocnieniu zarządzania stanem bezpieczeństwa danych, tak aby eliminować słabe punkty, poprawiać efektywność i budować trwałą odporność.

W obliczu rosnącej złożoności i ryzyka najnowsze technologie i narzędzia kształtują na nowo dyskusję o bezpieczeństwie danych. Wśród nich generatywna AI (GenAI) wyróżnia się jako pozytywny czynnik zmian, napędzający produktywność i innowacyjność. Jednak w miarę jak organizacje przyspieszają wdrażanie GenAI, dostrzegają również potrzebę bardziej rygorystycznych mechanizmów kontroli danych oraz zarządzania ładem danych.

W tym celu zespoły coraz częściej wykorzystują samo GenAI do wzmocnienia stanu zabezpieczeń danych — identyfikując ukryte zagrożenia, usprawniając operacje i skutecznie analizując ryzyka związane z danymi — przy czym coraz większą rolę odgrywają agenci AI i automatyzacja.

O BADANIU

Po raz trzeci z rzędu Microsoft zlecił firmie Hypothesis Group, niezależnej agencji badawczo-strategicznej, przeprowadzenie międzynarodowego badania wśród ponad 1700 specjalistów ds. bezpieczeństwa danych.

Inicjatywa Wskaźnik bezpieczeństwa danych została obecnie rozszerzona na 10 rynków: Stany Zjednoczone, LATAM (Brazylia), EMEA (Wielka Brytania, Niemcy, Francja) oraz APAC (Indie, Australia, Korea, Singapur, ZEA), aby lepiej zrozumieć potrzeby partnerów i klientów na całym świecie, gdy liderzy bezpieczeństwa danych opracowują własne strategie. Nowością w tegorocznych badaniach jest 10 pogłębionych wywiadów z liderami ds. bezpieczeństwa danych w USA i Wielkiej Brytanii, które mają na celu osadzenie wniosków w kontekście doświadczeń klientów.

Najważniejsze wnioski

01
Od rozdrobnionych narzędzi do ujednoliconego bezpieczeństwa danych

Klienci dążą do konsolidacji rozwiązań w celu poprawy bezpieczeństwa danych, widoczności danych oraz zarządzania nimi.

Organizacje priorytetowo traktują inwestycje w bezpieczeństwo danych, przechodząc od nadmiaru narzędzi do zintegrowanych platform. Coraz większy nacisk na Zarządzanie stanem bezpieczeństwa danych (DSPM) pomaga zespołom zwiększyć widoczność, ograniczyć złożoność i przejść na proaktywne zarządzanie ryzykiem dotyczącym danych.

86%
ankietowanych liderów preferuje zintegrowane platformy zamiast rozproszonych narzędzi, wskazując na lepszą przejrzystość, mniej alertów i większą efektywność.

80%+
ankietowanych organizacji wdraża lub rozwija strategie DSPM.

02
Bezpieczne zarządzanie produktywnością napędzaną AI

W miarę jak organizacje wdrażają rozwiązania GenAI w celu zwiększenia produktywności, rośnie zapotrzebowanie na solidniejszą ochronę danych.

Organizacje utrzymują równowagę między innowacjami AI a odpowiedzialnością. Wzrost liczby incydentów związanych z nieautoryzowanym wykorzystaniem AI wymusza wprowadzenie bardziej rygorystycznych kontroli, udoskonalenie polityk oraz ponowne skupienie się na edukacji pracowników i bezpiecznym zarządzaniu AI.

32%
zdarzeń zagrażających bezpieczeństwu danych w ankietowanych organizacjach dotyczy wykorzystania narzędzi GenAI.

47%
ankietowanych organizacji wdraża mechanizmy kontrolne GenAI (wzrost o 8 pp w porównaniu z 2024 r).

03
Wzmocnienie bezpieczeństwa danych dzięki GenAI

GenAI może być wykorzystany poprzez agentów i automatyzację do wzmocnienia programów bezpieczeństwa danych.

Liderzy ds. bezpieczeństwa danych coraz częściej wykorzystują GenAI do wzmacniania swoich programów bezpieczeństwa danych — automatyzując wykrywanie, usprawniając badania i zwiększając ochronę. Nadzór ludzki pozostaje kluczowy, gdy organizacje wdrażają agentów AI i automatyzację, aby skalować swoje działania w sposób bezpieczny i inteligentny.

82%
organizacji objętych badaniem opracowało plany wykorzystania GenAI w programach bezpieczeństwa danych (wzrost o 18 punktów procentowych w porównaniu z rokiem 2024).

39%
ankietowanych organizacji korzysta z agentów AI GenAI do celów bezpieczeństwa danych, a 58% ankietowanych deklaruje, że prowadzi testy lub eksploruje takie 58 proc.

1

Od rozdrobnionych narzędzi do ujednoliconego bezpieczeństwa danych

Klienci dążą do konsolidacji rozwiązań, aby poprawić bezpieczeństwo i widoczność danych oraz zarządzanie i nadzór

Organizacje priorytetowo traktują bezpieczeństwo danych jak nigdy dotąd, kierując nowe inwestycje na wzmocnienie swoich zabezpieczeń i umożliwienie bezpiecznych innowacji

88 proc. ankietowanych decydentów przewiduje, że ich budżety na bezpieczeństwo danych i zgodność z przepisami wzrosną w przyszłym roku. Ostatecznie celem tych inwestycji jest wyprzedzanie ryzyka związanego z danymi, ochrona danych wrażliwych oraz dbanie o odpowiedzialne korzystanie z GenAI — wszystko to przy jednoczesnym umożliwianiu innowacji.

Najważniejsze cele inwestycji w zwiększenie bezpieczeństwa danych

Osoby podejmujące decyzje dotyczące IT i bezpieczeństwa danych

Wyprzedzanie zmieniających się zagrożeń bezpieczeństwa danych	57%
Ochrona danych wrażliwych	56%
Umożliwianie bezpiecznych innowacji i wdrażania nowych technologii	53%
Zapewnienie bezpiecznego i odpowiedzialnego korzystania z narzędzi GenAI przez pracowników	52%

> „Gdyby mój zespół mógł wykonywać wszystkie codzienne zadania w jednym ekosystemie, ułatwiłoby nam to życie”.
>
> Dyrektor IT w sektorze produkcyjnym

Zespoły mają trudności z widocznością i nadzorem, ponieważ brakuje im ujednoliconego widoku zasobów danych

Decydenci wskazują, że ich największe wyzwania związane z widocznością danych dotyczą słabej integracji, braku spójnego widoku we wszystkich środowiskach oraz różnorodnych narzędzi. Jeden z liderów ds. bezpieczeństwa danych w sektorze finansowym i bankowym wyjaśnia: „Mamy słabą integrację narzędzi. Narzędzia nie zapewniają nam nadzoru, którego potrzebujemy. Nadal jest dużo wyników fałszywie dodatnich i alertów".

Te silosy utrudniają zespołom łączenie informacji, korelowanie zdarzeń i utrzymanie widoczności w środowiskach roboczych.

Główne wyzwania dotyczące widoczności danych

Osoby podejmujące decyzje dotyczące IT i bezpieczeństwa danych

Kiepska integracja z platformami bezpieczeństwa i zarządzania danymi	29%
Brak ujednoliconego widoku w różnych środowiskach	25%
Rozproszone narzędzia bez scentralizowanego pulpitu zarządczego	23%

Liderzy odpowiadają poprzez konsolidację narzędzi i inwestowanie w zintegrowane platformy, które upraszczają działania, jednocześnie poprawiając widoczność i kontrolę

86 proc. ankietowanych osób decyzyjnych zgadza się, że kompleksowa platforma zabezpieczeń ze zintegrowanymi rozwiązaniami przewyższa możliwości korzystania z wielu najlepszych w swojej klasie rozwiązań, które wymagają ręcznej integracji i ręcznego zarządzania. Korzyści płynące z konsolidacji są oczywiste: zastosowanie jednolitego podejścia umożliwia skuteczniejsze wykrycie ryzyka i reagowanie na ryzyka związane z danymi, prostsze zarządzanie przez zespoły ds. bezpieczeństwa danych oraz lepszą widoczność ryzyk związanych z danymi.

> „Staramy się korzystać z mniejszej liczby dostawców. Jeśli potrzebujemy 15 narzędzi, wolelibyśmy nie zarządzać rozwiązaniami od 15 różnych dostawców. Wolelibyśmy ograniczyć tę liczbę do pięciu, przy czym każdy dostawca obsługuje trzy narzędzia”.
>
> Globalny dyrektor ds. bezpieczeństwa informacji Branża turystyczna

Najważniejsze korzyści konsolidacji

Osoby podejmujące decyzje dotyczące IT i bezpieczeństwa danych

Skuteczniejsze wykrywanie zagrożeń i reagowanie na nie

Łatwiejsze zarządzanie i utrzymanie narzędzi przez zespół ds. bezpieczeństwa danych

Lepsza widoczność ryzyka związanego z danymi w różnych obciążeniach

Dążenie do integracji przyspieszyło wdrażanie strategii Zarządzania stanem bezpieczeństwa danych (DSPM)

Większość ankietowanych organizacji informuje, że już opracowuje lub wdraża strategie DSPM (czyli ramy zapewniające jednolitą widoczność, ciągłą ocenę ryzyka danych oraz egzekwowanie polityk w środowiskach danych), w tym:

Identyfikacja i priorytetyzacja zagrożeń związanych z ujawnieniem danych lub nieprawidłową konfiguracją	82%
Wykrywanie, kto, kiedy oraz jak uzyskuje dostęp do danych wrażliwych	81%
Definiowanie i egzekwowanie zasad zabezpieczeń danych	80%
Odkrywanie i klasyfikowanie danych wrażliwych w różnych środowiskach	79%

Budując zintegrowane ekosystemy i włączając DSPM do kluczowych procesów, organizacje zmierzają w kierunku przyszłości, w której widoczność i ochrona danych nie będą już rozproszonymi działaniami, lecz elementem bardziej spójnej strategii bezpieczeństwa danych.

„Powiedziałbym, że mamy całkiem dobrą strategię DSPM. Integrujemy DPSM z zarządzaniem tożsamościami, dzięki czemu nie tylko wiemy, gdzie znajdują się dane, ale możemy również zapewnić, że dostęp do nich mają wyłącznie odpowiednie osoby. Dla nas najważniejsze jest posiadanie proaktywnej, realizowanej w czasie rzeczywistym możliwości identyfikowania danych wymagających ochrony, a następnie stosowania wobec nich naszego systemu kontroli. DSPM umożliwia bardziej zautomatyzowane stosowanie i zarządzanie kontrolami”.

Globalny dyrektor ds. bezpieczeństwa informacji
Branża turystyczna

Droga przed nami

Rosnąca ilość danych i narzędzi sprawiła, że widoczność i zarządzanie stały się coraz bardziej złożone. Aby przezwyciężyć te wyzwania, organizacje muszą wytyczyć ścieżkę prowadzącą do konsolidacji, integracji i proaktywnego DSPM.

01

Zintegruj bezpieczeństwo danych, widoczność i zarządzanie danymi.

Zdecydowana większość ankietowanych liderów zgadza się, że zintegrowane platformy przewyższają rozproszone zestawy narzędzi. Konsolidacja upraszcza nadzór, zwiększa widoczność oraz wzmacnia wykrywanie zagrożeń i reakcję na nie. Organizacje powinny koncentrować się na budowie ekosystemów, w których bezpieczeństwo danych, zgodność i IT funkcjonują w ramach jednej, zintegrowanej struktury.

02

Wykorzystaj Zarządzanie stanem bezpieczeństwa danych (DSPM) jako narzędzie ułatwiające większą widoczność i ochronę.

DSPM umożliwia przejście od reaktywnej ochrony do proaktywnego zarządzania ryzykiem danych. Inwestując w strategie DSPM, zespoły mogą identyfikować i priorytetyzować ryzyka związane z danymi, monitorować dostęp do danych wrażliwych oraz wdrażać spójne polityki w środowiskach wielochmurowych.

03

Kształtuj wspólną odpowiedzialność za stan zabezpieczeń danych.

Ustanowienie jasnej odpowiedzialności w zakresie IT i operacji zabezpieczeń w celu ochrony danych wrażliwych oraz koordynowania ich przepływu pomiędzy jednostkami biznesowymi. Współpraca między zespołami IT, ds. zgodności i bezpieczeństwa jest kluczowa dla budowania trwałej odporności w coraz bardziej złożonym środowisku danych.

2

Bezpieczne zarządzanie produktywnością napędzaną AI

W miarę jak organizacje wdrażają rozwiązania GenAI w celu zwiększenia produktywności, rośnie zapotrzebowanie na solidniejszą ochronę danych

Generatywna AI (GenAI) szybko zmienia sposób pracy pracowników, wywołując nową falę kreatywności, produktywności i innowacji — ale organizacje nie są naiwne wobec potencjalnych zagrożeń dla danych, zwłaszcza wynikających z nieautoryzowanego użycia GenAI

Pracownicy z entuzjazmem korzystają z GenAI; według wskaźnika trendów w pracy na rok 2025 większość ankietowanych globalnych pracowników wiedzy deklaruje korzystanie z AI, a ponad 70 proc. deklaruje, że przynosi własne narzędzia AI do pracy[1] — co świadczy o rosnącym trendzie wykorzystywania narzędzi AI w miejscu pracy.

Jednak wraz z przyspieszeniem wdrażania AI, dyskusja coraz bardziej koncentruje się na odpowiedzialnym użytkowaniu, a nie tylko na umożliwieniu korzystania z tych narzędzi. Liderzy rozumieją, że te same technologie, które zwiększają produktywność, wprowadzają także nowe ryzyka dla bezpieczeństwa danych — zwłaszcza gdy pracownicy eksperymentują z GenAI bez nadzoru lub zgody.

1. Microsoft, 2025, Trendy na rynku pracy

70+%

ankietowanych pracowników wiedzy używających AI przynosi własne narzędzia AI do pracy[1]

32%

zdarzeń zagrażających bezpieczeństwu danych w ankietowanych organizacjach dotyczy wykorzystania narzędzi GenAI

Według ankietowanych organizacji jedna trzecia (32 proc.) zdarzeń zagrażających bezpieczeństwu danych wiąże się z wykorzystaniem narzędzi GenAI, a 35 proc. przewiduje większą liczbę incydentów w nadchodzącym roku z powodu użycia GenAI. Największą obawą nie jest sama technologia, lecz to, w jaki sposób i gdzie pracownicy ją wykorzystują. Wielu pracowników korzysta z konsumenckich narzędzi GenAI lub loguje się przy użyciu prywatnych danych uwierzytelniających, omijając w ten sposób korporacyjne zabezpieczenia i nadzór.

Ankietowani decydenci ds. bezpieczeństwa danych wskazują, że:

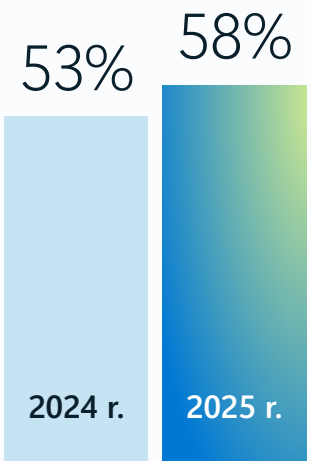
- Odsetek pracowników korzystających z prywatnych danych uwierzytelniających do uzyskiwania dostępu do GenAI w celach służbowych wzrósł o 5 punktów procentowych rok do roku.
- Liczba pracowników korzystających z urządzeń prywatnych w celu uzyskania dostępu do GenAI w celach służbowych wzrosła o 9 punktów procentowych w ujęciu rok do roku.

> „Nie chcemy, aby poufne lub zastrzeżone dane opuszczały zaporę sieciową — a tak właśnie się dzieje, jeśli pracownicy korzystają z niesankcjonowanych narzędzi GenAI".
>
> Globalny dyrektor ds. bezpieczeństwa informacji Branża turystyczna

Takie zachowania mogą narazić dane wrażliwe na kontakt z systemami zewnętrznymi, przez co organizacje nie wiedzą, dokąd przepływają informacje i kto ma do nich dostęp. Kompromis między produktywnością a bezpieczeństwem jest realny — zespoły chcą wspierać innowacyjność, ale nie kosztem bezpieczeństwa danych ani zgodności z przepisami.

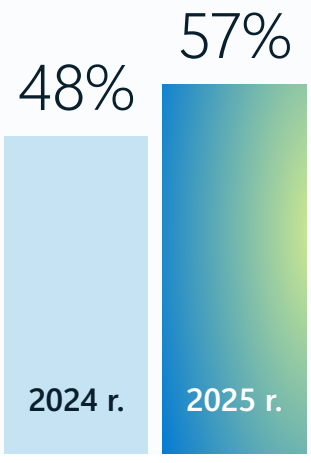
Odsetek pracowników korzystających z prywatnych poświadczeń do uzyskania dostępu do GenAI w pracy

Osoby podejmujące decyzje dotyczące IT i bezpieczeństwa danych



Odsetek pracowników korzystających z urządzeń osobistych do uzyskiwania dostępu do GenAI w pracy

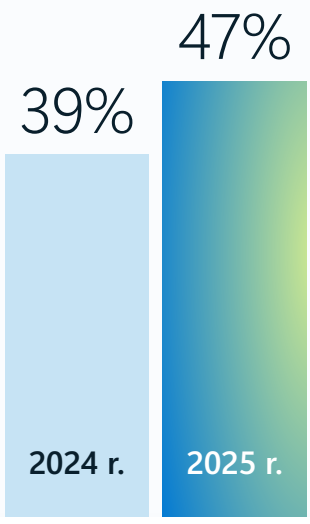
Osoby podejmujące decyzje dotyczące IT i bezpieczeństwa danych



W obliczu tych wyzwań zespoły ds. bezpieczeństwa danych podejmują zdecydowane działania, aby wzmocnić kontrolę nad wykorzystaniem GenAI przez pracowników

Prawie połowa (47%) ankietowanych organizacji wdraża konkretne mechanizmy kontroli AI w 2025 roku, w porównaniu do 39% w roku poprzednim — to znaczący wzrost, odzwierciedlający narastającą pilność.

% ankietowanych organizacji wdrażających konkretne kontrole GenAI



Najważniejsze priorytety w zakresie kontroli GenAI

Osoby podejmujące decyzje dotyczące IT i bezpieczeństwa danych

Zapobieganie przesyłaniu danych wrażliwych do narzędzi GenAI	42%
Szkolenie pracowników w zakresie bezpiecznego korzystania z narzędzi GenAI	38%
Wykrywanie nietypowej aktywności użytkowników i identyfikacja ryzykownych użytkowników	37%
Identyfikowanie wrażliwych danych przesyłanych do lub generowanych przez narzędzia GenAI	37%

> „Pracujemy nad blokowaniem nieautoryzowanych narzędzi GenAI, a także nad rozszerzaniem zakresu autoryzowanych narzędzi i kierowaniem użytkowników do nich”.
>
> CISO, opieka zdrowotna i farmacja

Wdrożenie tych mechanizmów kontroli ostatecznie pomaga liderom ds. bezpieczeństwa danych zyskać większą pewność siebie. Poza technologią, decydenci zachęcają pracowników do korzystania z zatwierdzonych narzędzi AI, wzmacniają bezpieczne praktyki oraz tworzą przejrzyste procesy zatwierdzania. Wiadomość jest jasna: celem nie jest ograniczanie innowacji — lecz zapewnienie jej bezpiecznego rozwoju.

Droga przed nami

W miarę jak GenAI staje się coraz bardziej powszechnym elementem codziennych działań, organizacje muszą znaleźć równowagę między dążeniem do produktywności a solidnym zarządzaniem i kontrolą. Przyszłość bezpiecznego wdrażania AI zależeć będzie od przejrzystości, edukacji i proaktywnego zarządzania ryzykiem danych.

01

Zwiększ widoczność i kontrolę nad użyciem GenAI.

Organizacje powinny wdrażać narzędzia bezpieczeństwa danych, które potrafią wykrywać i chronić użycie aplikacji GenAI w całym przedsiębiorstwie, umożliwiając analizę tego, które narzędzia są wykorzystywane, jakie przepływy danych przez nie występują oraz gdzie występują potencjalne zagrożenia. Ciągłe monitorowanie umożliwia zespołom ds. bezpieczeństwa identyfikację nieautoryzowanego użycia, zanim przerodzi się ono w incydent bezpieczeństwa danych.

02

Zapobiegaj ekspozycji danych poprzez proaktywne zasady ochrony.

Jednym z najskuteczniejszych zabezpieczeń jest zapobieganie przedostawaniu się danych wrażliwych do narzędzi GenAI. Ustanów zasady ograniczające typy danych, które mogą być przetwarzane przez aplikacje GenAI, oraz wdroż zautomatyzowane mechanizmy kontroli blokujące ryzykowne przesyłanie danych lub podejmowanie działań w czasie rzeczywistym.

03

Edukuj i motywuj pracowników.

Sama technologia nie rozwiąże wyzwania związanego z zarządzaniem. Ciągła edukacja pracowników — uzupełniona jasnymi wskazówkami dotyczącymi zatwierdzonych narzędzi i praktyk — pomaga kształtować kulturę odpowiedzialnego korzystania z GenAI. Przejrzystość buduje zaufanie, umożliwiając zespołom wykorzystanie pełnego potencjału GenAI bez naruszania bezpieczeństwa danych.

3

Wzmocnienie bezpieczeństwa danych dzięki GenAI

GenAI może być wykorzystany poprzez agentów i automatyzację do wzmocnienia programów bezpieczeństwa danych

Organizacje przyspieszają wdrażanie GenAI w programach bezpieczeństwa danych, aby zmaksymalizować produktywność i efektywność

Coraz więcej organizacji decyduje się na wykorzystanie GenAI w celu wzmocnienia swoich programów bezpieczeństwa danych — wykorzystując tę technologię do szybszego wykrywania ryzyk, zarządzania większymi wolumenami danych oraz precyzyjnego dostosowywania zasad ochrony. W 2025 roku 82 proc. ankietowanych organizacji informuje, że opracowało plany wykorzystania GenAI w swoich operacjach zabezpieczeń danych, co stanowi znaczący wzrost w porównaniu do 64 proc. w 2024 roku.

Wzrost adopcji świadczy o rosnącym zaufaniu liderów, że GenAI może pomóc wymocnić a nie osłabić, ich ogólny stan zabezpieczeń. Wielu z nich wdraża GenAI zarówno do proaktywnych przypadków użycia, takich jak ocena i zabezpieczanie środowisk danych oraz ulepszanie polityki bezpieczeństwa, jak również do reaktywnych przypadków użycia, takich jak wykrywanie danych wrażliwych, identyfikacja krytycznych zagrożeń i badanie potencjalnych zdarzeń zagrażających bezpieczeństwu.

82%

ankietowanych organizacji zgłasza, że opracowało plany wykorzystania GenAI w operacjach zabezpieczeń danych (w porównaniu do 64% w 2024 roku)

Główne obszary wykorzystania GenAI w bezpieczeństwie danych

Osoby podejmujące decyzje dotyczące IT i bezpieczeństwa danych

Wykrywanie danych wrażliwych	44%
Wykryj krytyczne ryzyka bezpieczeństwa danych	43%
Badanie potencjalnych incydentów	43%
Ocena stanu zabezpieczeń środowisk danych	42%
Zabezpiecz środowisko danych	41%
Dopracuj zasady dotyczące bezpieczeństwa danych	38%

> „Nasze systemy GenAI nieustannie obserwują, uczą się i formułują zalecenia dotyczące modyfikacji, wykorzystując o wiele większą ilość danych, niż byłoby to możliwe w przypadku jakiegokolwiek procesu manualnego lub półmanualnego”.
>
> Dyrektor IT w sektorze energetycznym

> „Powiedziałbym, że udało nam się ograniczyć ręczne prace związane z programem bezpieczeństwa danych o co najmniej 40 proc. Udoskonaliliśmy nasze procesy bardziej niż wcześniej wspomniano, prawdopodobnie o ponad 50 proc. Nasze programy GenAI automatyzują rutynowe zadania i uczą się na podstawie zmieniających się zagrożeń".
>
> Starszy wiceprezes ds. cyberbezpieczeństwa, chmury i zarządzania ryzykiem stron trzecich w finansach i bankowości

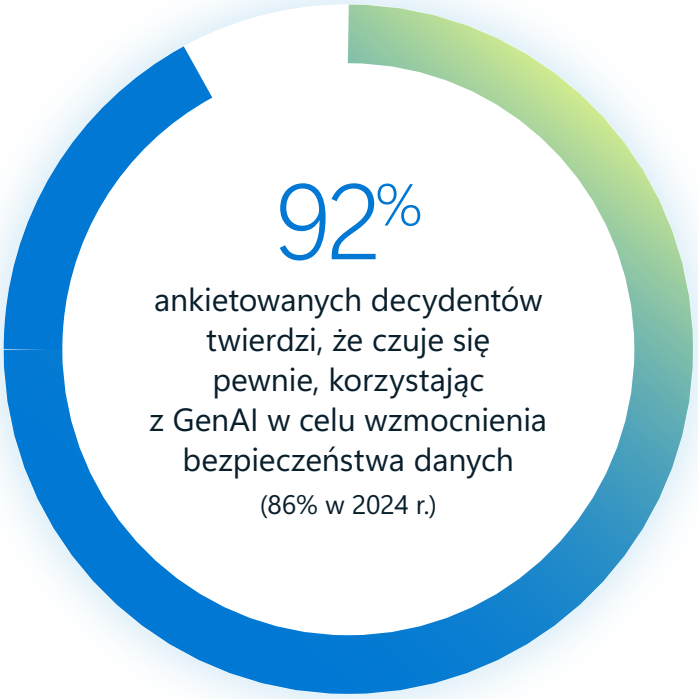
Automatyzując rutynowe zadania związane z bezpieczeństwem danych i przyspieszając wykrycie ryzyka oraz reagowanie na zagrożenia, GenAI umożliwia zespołom efektywniejszą pracę przy ograniczonych zasobach. Decydenci wskazują kluczowe korzyści, takie jak poprawa efektywności, lepsza adaptacja do zmieniających się zagrożeń, odciążenie zespołów na rzecz bardziej strategicznej pracy oraz analiza większej ilości danych niż pozwalają na to tradycyjne narzędzia.

W jakim obszarze GenAI przynosi największy wpływ w programach bezpieczeństwa danych

Osoby podejmujące decyzje dotyczące IT i bezpieczeństwa danych

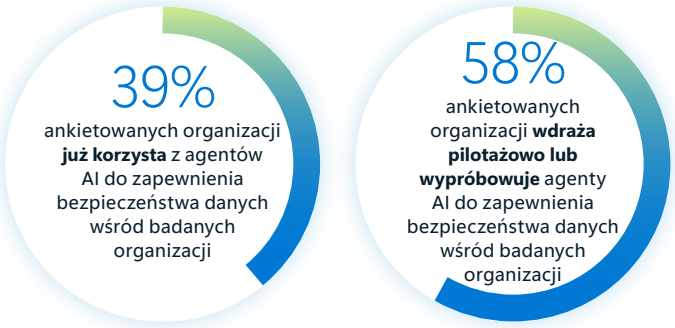
Zautomatyzuj rutynowe zadania związane z bezpieczeństwem, aby zwiększyć wydajność	**38%**
Zwiększenie naszej zdolności do adaptacji i uczenia się w odpowiedzi na ewoluujące zagrożenia	**36%**
Umożliwienie naszemu zespołowi ds. bezpieczeństwa danych poświęcania więcej czasu na zadania strategiczne	**35%**
Analizuj więcej danych niż byłoby to możliwe w przypadku innych rozwiązań	**35%**

Zaufanie do rozwiązań bezpieczeństwa opartych na GenAI szybko rośnie. Dziewięćdziesiąt dwa procent ankietowanych decydentów deklaruje, że czuje się pewnie, wykorzystując GenAI do wzmocnienia bezpieczeństwa danych — to wzrost w porównaniu z 86 proc. w 2024 r.



Agenty AI są uznawane za kluczową szansę dla programów bezpieczeństwa danych, ale wymagają nadzoru ludzkiego

Rosnąca popularność GenAI w programach bezpieczeństwa danych obejmuje również pojawienie się agentów GenAI — inteligentnych systemów zdolnych do wykrywania krytycznych zagrożeń, automatycznej klasyfikacji lub ochrony danych oraz rekomendowania środków kontrolnych w czasie rzeczywistym. 39 proc. ankietowanych organizacji stwierdziło, że już korzysta z agentów GenAI do ochrony danych, podczas gdy kolejne 58 proc. poinformowało, że je testuje lub rozważa ich wdrożenie.



> „Obecnie mamy wdrożoną Agentic AI w niektórych naszych narzędziach bezpieczeństwa. Nasze rozwiązanie do szkolenia testerów i zwiększania świadomości na temat phishingu wykorzystuje Agentic AI do analizy nowych zagrożeń w czasie rzeczywistym oraz zachowań użytkowników".
>
> Globalny dyrektor ds. bezpieczeństwa informacji Branża turystyczna

Najważniejsze przypadki użycia agentowych rozwiązań AI w zakresie bezpieczeństwa danych

Osoby podejmujące decyzje dotyczące IT i bezpieczeństwa danych

Wykryj krytyczne ryzyka	**40%**
Automatycznie chroń, blokuj, oznaczaj i klasyfikuj dane	**36%**
Zbadaj potencjalne incydenty dotyczące bezpieczeństwa danych	**35%**
Zalecenia dotyczące lepszego zabezpieczenia środowiska danych	**35%**
Ograniczenie liczby fałszywych alertów	**35%**

Mimo to, nawet gdy organizacje wdrażają te możliwości, liderzy podkreślają znaczenie zachowania nadzoru człowieka nad procesem. 38 proc. ankietowanych decydentów wyraża obawy dotyczące korzystania przez pracowników z agentów AI bez odpowiedniego zezwolenia lub nadzoru człowieka.

Dyrektor ds. globalnego cyberbezpieczeństwa w branży produkcyjnej wyjaśnia: „Mamy agentów AI do różnych zastosowań, ale wciąż jest człowiek w procesie, który nadzoruje ich pracę i sprawdza uzyskane dane".

Automatyzacja i agenci GenAI już przekształcają bezpieczeństwo danych — nie zastępując ludzkiego osądu, lecz go wzmacniając. Zwiększają zasięg działania zespołów ds. bezpieczeństwa, umożliwiając im szybszą reakcję i dostosowywanie się do zmieniających się zagrożeń. Jednak wraz ze wzrostem skali tych rozwiązań, niezbędne są silne mechanizmy ochronne, aby szybkość nie prowadziła do naruszenia zabezpieczeń ani utraty zaufania.

Droga przed nami

Organizacje integrują GenAI jako podstawę swoich programów bezpieczeństwa danych. Kolejny etap dojrzałości polega na wykorzystaniu GenAI do automatyzacji i zwiększania ochrony oraz przyspieszania badań — co pomaga zespołom bezpiecznie skalować działania i wyprzedzać zmieniające się zagrożenia.

01

Zintegruj GenAI z workflow bezpieczeństwa danych.

Wdrożenie GenAI w procesach wykrywania, badania i polityki zwiększa przejrzystość, priorytetyzację i szybkość reakcji. GenAI może priorytetyzować alerty, korelować zdarzenia oraz ujawniać istotne informacje, które pomagają zespołom skupić się na najważniejszych zagrożeniach.

02

Użyj agentów AI GenAI, aby przyspieszyć reakcję i zredukować szum.

Agenci GenAI oferują skalowalną automatyzację w zakresie odnajdowania danych, ochrony i reagowania na incydenty. Jeśli zostaną wdrożone z rozwagą, mogą pomóc ograniczyć nakład pracy ręcznej i poprawić spójność bez uszczerbku dla kontroli.

03

Utrzymuj nadzór ludzki, aby zachować kontrolę.

Ludzka wiedza i doświadczenie pozostają niezbędne do kierowania, weryfikowania i udoskonalania wyników osiąganych dzięki GenAI. Jasne ramy zarządzania oraz procesy weryfikacji ręcznej mają kluczowe znaczenie dla zapewnienia dokładności, uczciwości i zaufania do operacji zabezpieczeń obsługiwanych przez GenAI.

Zalecenia końcowe

Integracja zapewniająca większą widoczność: zintegrowane platformy kluczem do silniejszej ochrony

W miarę jak wolumen danych nadal rośnie, widoczność pozostaje jednym z największych wyzwań w ochronie informacji wrażliwych. Organizacje nie mogą już sobie pozwolić na zarządzanie dziesiątkami niepowiązanych ze sobą narzędzi, które powodują luki w widoczności i zwiększają obciążenie operacyjne. Przejście na zintegrowaną platformę, wspieraną przez DSPM, zapewnia jednolitą widoczność i kontrolę niezbędną do ograniczenia złożoności i wzmocnienia ochrony. Skonsolidowane, spójne podejście pomaga organizacjom nie tylko usprawnić zarządzanie, ale także zwiększyć skuteczność wykrywania i reagowania — zamieniając widoczność w odporność.

Pozostań produktywny, pozostań bezpieczny: opanowanie równowagi bezpieczeństwa GenAI

W miarę jak GenAI staje się nieodłącznym elementem codziennej pracy, wyzwaniem dla organizacji nie jest to, czy z niego korzystać, lecz jak korzystać z niego bezpiecznie. Wzrost nieautoryzowanego lub niezarządzanego korzystania z GenAI podkreśla potrzebę większego nadzoru i zarządzania zgodnością. Kluczowymi krokami w ograniczaniu ryzyka są wdrożenie mechanizmów kontroli zapobiegających przedostawaniu się danych wrażliwych do narzędzi GenAI, identyfikacja wykorzystania GenAI w różnych środowiskach oraz szkolenie pracowników w zakresie bezpiecznych praktyk. Wprowadzając właściwe mechanizmy kontroli, GenAI może nadal napędzać innowacje bez naruszenia zabezpieczeń danych ani zgodności.

Inteligentniej, szybciej, bezpieczniej: rewolucjonizowanie bezpieczeństwa danych dzięki GenAI

GenAI radykalnie zmienia sposób, w jaki organizacje wykrywają, reagują i zapobiegają zagrożeniom dla danych. Włączenie GenAI do procesów bezpieczeństwa umożliwia zespołom automatyzację rutynowych zadań, szybszą analizę złożonych danych oraz prowadzenie bardziej zaawansowanych badań. W miarę jak organizacje wdrażają agentów AI GenAI i automatyzację w celu skalowania swoich programów bezpieczeństwa danych, nadzór ludzki pozostaje niezbędny. Najskuteczniejsze strategie ochrony danych będą łączyć analityczne możliwości GenAI z ludzkim osądem, aby działać szybciej, eliminować zakłócenia i ograniczać ryzyko ekspozycji danych.

Cele badania

Zrozum krajobraz bezpieczeństwa danych, w tym priorytety i podejścia, wyzwania oraz przyczyny i skutki zdarzeń zagrażających bezpieczeństwu danych.

Przyjrzyj się przyszłości bezpieczeństwa danych, nowo pojawiającym się strategiom i innowacjom oraz planom organizacji dotyczącym inwestycji w przyszłość.

Poznaj wpływ wykorzystania GenAI przez pracowników na bezpieczeństwo danych oraz sposoby, w jakie zespoły używają GenAI w swoich programach bezpieczeństwa danych.

Metodologia

Pomiędzy 16 lipca a 11 sierpnia 2025 r. przeprowadzono 25-minutową międzynarodową ankietę online wśród 1,725 liderów w zakresie bezpieczeństwa danych.

Pytania dotyczyły sytuacji w zakresie bezpieczeństwa danych, zdarzeń zagrażających bezpieczeństwu, zabezpieczania korzystania z GenAI przez pracowników oraz wykorzystania GenAI w programach bezpieczeństwa danych w celu porównania z 2024 rokiem.

Przeprowadzono godzinne, pogłębione wywiady z 10 liderami ds. bezpieczeństwa danych w USA i Wielkiej Brytanii, aby poznać historie o tym, jak podchodzą oni do kwestii bezpieczeństwa danych w swoich organizacjach.

Grupa docelowa respondentów

Liderzy w zakresie bezpieczeństwa danych musiały spełniać następujące kryteria wyboru:

- być CISO i podobnymi decydentami (poziom C-2 i wyższy), których zadaniem jest bezpieczeństwo danych
- Praca w dużych organizacjach (ponad 500 pracowników, różne wielkości)
- Mieszanka branż regulowanych lub nieuregulowanych (innych niż organizacje edukacyjne, instytucje rządowe lub organizacje non-profit)

Spośród 1,725 ankietowanych liderów w zakresie bezpieczeństwa danych kompletne dane według kraju były następujące:

- Stany Zjednoczone: 300
- Zjednoczone Królestwo: 300
- Indie: 300
- Francja: 150
- Niemcy: 150
- Brazylia: 150
- Australia: 150
- ZEA: 75
- Korea: 75
- Singapur: 75

hypothesis Microsoft Security

Załącznik

Ujednolicenie ochrony danych i innowacji związanych z AI w różnych regionach

Na całym świecie występują unikalne różnice w zakresie zaufania, gotowości i oczekiwań dotyczących GenAI i bezpieczeństwa danych

Stany Zjednoczone

Potrzeba wsparcia w obliczu rosnącej presji

+9%
Nadmierna presja na udowodnienie zwrotu z inwestycji w bezpieczeństwo danych

+15%
Przewiduje się wzrost liczby zdarzeń zagrażających bezpieczeństwu danych w wyniku korzystania przez pracowników z GenAI

+6%
Większe trudności z niedokładną/niekompletną klasyfikacją danych

+5%
Większe trudności w zarządzaniu DSPM ze względu na zbyt wiele niezintegrowanych narzędzi

Ameryka Łacińska

Akceptacja wzrostu przy zachowaniu kontroli

+7%
Częściej spodziewają się wzrostu budżetów na bezpieczeństwo danych

+14%
Organizacje są bardziej skłonne mieć w pełni wdrożoną strategię DSPM

+7%
Więcej kontroli nad korzystaniem przez pracowników z GenAI

EMEA

Mniej dojrzałe w zarządzaniu ryzykiem związanym z danymi GenAI i wykorzystywaniu Agentic AI

–5%
W mniejszym stopniu obawiają się niemożności ochrony danych trafiających do aplikacji/narzędzi GenAI

–4%
Rzadziej występują mechanizmy kontroli identyfikujące ryzykownych użytkowników korzystających z aplikacji/narzędzi GenAI

–4%
Mniejsze wykorzystanie agentów GenAI do ochrony danych

Azja i Pacyfik

Borykają się z wysokim wskaźnikiem incydentów

+45
Więcej incydentów związanych z bezpieczeństwem danych w ostatnich 12 miesiącach

+4 dni
Więcej czasu na wykrywanie i reagowanie

+5%
Rosnące zapotrzebowanie na specjalistów ds. bezpieczeństwa danych do efektywnego zarządzania obowiązkami

+5%
Aplikacje GenAI częściej są przedmiotem naruszenia zabezpieczeń w zdarzeniach zagrażających bezpieczeństwu danych

Przedstawione luki odzwierciedlają różnice pomiędzy danymi regionalnymi a danymi globalnymi