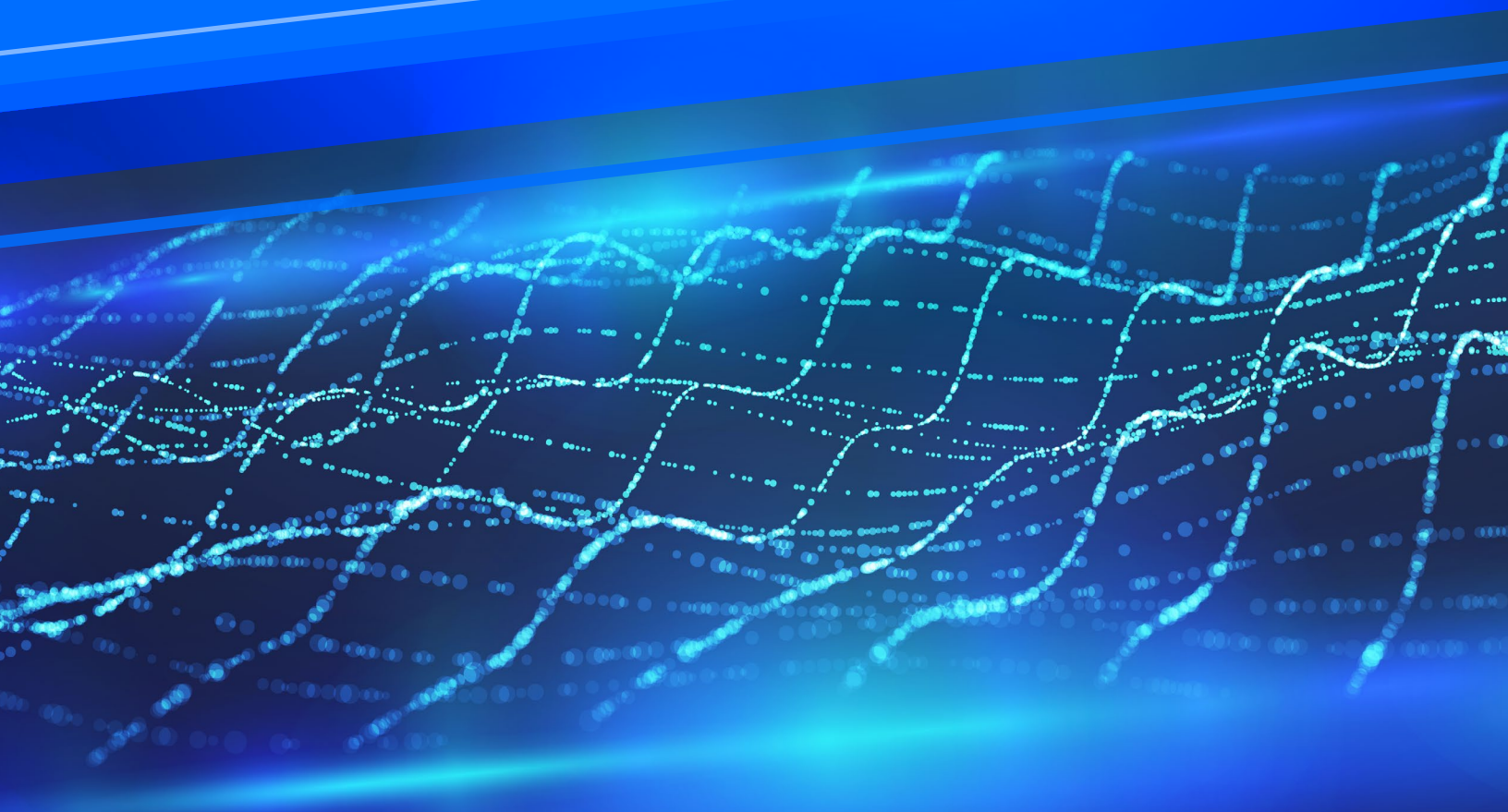
Bitdefender

Bitdefender - Ocena stanu cyberbezpieczeństwa 2026

Globalne wnioski na podstawie opinii 1 200 specjalistów IT i cyberbezpieczeństwa



KLUCZOWE WNIOSKI

SEKCJA 1

SEKCJA 2

SEKCJA 3

SEKCJA 4

SEKCJA 5

SEKCJA 6

SEKCJA 7

SEKCJA 8

PODSUMOWANIE

Najważniejsze wnioski w skrócie

Cyberbezpieczeństwo to proces, a nie cel sam w sobie. Na tej drodze pojawiają się kolejne etapy, które pokazują postępy, wyzwania i nowe możliwości.

Poniższe dane przedstawiają najważniejsze wnioski płynące z opinii specjalistów IT i cyberbezpieczeństwa na temat obecnej sytuacji, co najbardziej ich niepokoi, jakie przeszkody utrudniają skuteczną ochronę oraz w jakim kierunku, ich zdaniem, zmierza branża.

UJAWNIANIE NARUSZEŃ BEZPIECZEŃSTWA

55.2%
respondentów przyznało, że polecono im nie ujawniać informacji o naruszeniu bezpieczeństwa

ZAGROŻENIA I NARZĘDZIA

70.1%
obserwuje coraz bardziej zaawansowane ataki phishingowe

59%
zgłasza zastrzeżenia dotyczące swoich rozwiązań EDR/XDR

SZTUCZNA INTELIGENCJA

47.4%
nie ma pełnej widoczności wykorzystania narzędzi Shadow AI przez pracowników

52.6%
uważa, że sztuczna inteligencja bardziej wspiera cyberprzestępców niż obrońców

OPERACJE I ZAKRES OCHRONY

47.6%
nie jest w stanie zapewnić całodobowego monitorowania bezpieczeństwa (24/7)

61.5%
twierdzi, że niedobór specjalistów wynika z innych czynników niż brak kandydatów

48.7%
przyznaje, że ma trudności z zachowaniem równowagi między restrykcjami bezpieczeństwa a produktywnością pracowników

ZGODNOŚĆ Z PRZEPISAMI I SUWERENNOŚĆ DANYCH

76.1%
wskazuje, że suwerenność danych staje się jednym z kluczowych kryteriów przy podejmowaniu decyzji zakupowych

61.6%
uważa, że wymagania związane ze zgodnością z przepisami są przytłaczające

Podsumowanie dla kadry zarządzającej

Trzy sprzeczności definiują cyberbezpieczeństwo w 2026 roku. Organizacje są bardziej pewne siebie, ale liczba naruszeń pozostaje wysoka. Zagrożenia AI są już faktem, jednak większość zespołów nie widzi własnej ekspozycji na ryzyko AI. Znane wektory ataków są dobrze opisane, lecz nadal zbyt często ignorowane. To nie tylko luki w zabezpieczeniach. Pokazują, co dzieje się, gdy fascynacja nowymi technologiami przesłania podstawy cyberbezpieczeństwa – dokładnie na to liczą cyberprzestępcy.

To czwarta edycja raportu Bitdefender Cybersecurity Assessment, oparta na niezależnym badaniu 1 200 specjalistów IT i cyberbezpieczeństwa. Badanie objęło menedżerów średniego i wyższego szczebla oraz specjalistów odpowiedzialnych za codzienną ochronę organizacji. Respondenci pochodzili z sześciu krajów: Francji, Niemiec, Włoch, Singapuru, Wielkiej Brytanii i Stanów Zjednoczonych.

Wyniki ujawniają wyraźną różnicę między oceną poziomu bezpieczeństwa przez kierownictwo a opinią osób odpowiedzialnych za jego realizację. To jeden z najważniejszych wniosków raportu. Kadra zarządzająca konsekwentnie patrzy na poziom bezpieczeństwa bardziej optymistycznie niż praktycy wdrażający jej strategie.

Kolejny ważny wniosek: rosnące znaczenie niezależności danych coraz silniej wpływa na decyzje zakupowe.

Porównaliśmy również wyniki rok do roku i zaobserwowaliśmy wyraźne trendy. Odsetek ukrywanych naruszeń pozostaje wysoki mimo nowych obowiązków raportowania. Zagrożenia AI przestały być hipotetyczne i stały się rzeczywistością. Organizacje nadal zmagają się z wymaganiami zgodności, zbyt złożonymi środowiskami bezpieczeństwa oraz rosnącą powierzchnią ataku.

Analiza danych za 2026 rok pokazuje, że najlepiej chronione są nie organizacje z największą liczbą narzędzi lub najgłośniejszą strategią AI, lecz te, które ograniczają złożoność, odzyskują pełną widoczność i koncentrują się na skutecznym zapobieganiu atakom.

SEKCJA 1

Luka w ujawnianiu incydentów

Jeśli zapytasz liderów bezpieczeństwa, czy kiedykolwiek polecono im nie ujawniać naruszenia (my to zrobiliśmy), ponad połowa odpowie twierdząco.
Odsetek ten praktycznie się nie zmienił mimo nowych przepisów nakazujących zgłaszanie incydentów.

Utrzymywanie się tego wyniku wskazuje na problem głębszy niż same regulacje. Pokazuje, że utrwalona kultura organizacyjna wciąż opiera się zmianom, mimo nowych wymogów prawnych.

55.2%

respondentów przyznało, że polecono im zachować naruszenie w tajemnicy

Liczba, która pozostaje niezmienna

W 2023 roku po raz pierwszy zapytaliśmy specjalistów ds. bezpieczeństwa, czy kiedykolwiek polecono im zachować naruszenie w tajemnicy, mimo że powinno zostać zgłoszone. 42% odpowiedziało twierdząco. W 2025 roku odsetek ten wzrósł do 57,6%. W tym roku, wśród wszystkich 1 200 respondentów, wynosi 55,2%. Ta stabilizacja jest równie niepokojąca jak wcześniejszy gwałtowny wzrost.

Przepisy SEC dotyczące ujawniania incydentów cyberbezpieczeństwa weszły w życie w Stanach Zjednoczonych w 2023 roku. Dyrektywa NIS2 zaczęła obowiązywać w Europie w 2024 roku, a rozporządzenie DORA weszło w życie na początku 2025 roku. Mimo to odsetek prób ukrywania naruszeń praktycznie się nie zmienił.

Można to interpretować na kilka sposobów. Optymistyczna wersja zakłada, że obowiązek zgłaszania incydentów powstrzymał dalszy wzrost tego wskaźnika. Mniej optymistyczna wskazuje, że regulacje wciąż zmagają się z utrwalonymi przez dekady nawykami organizacji.

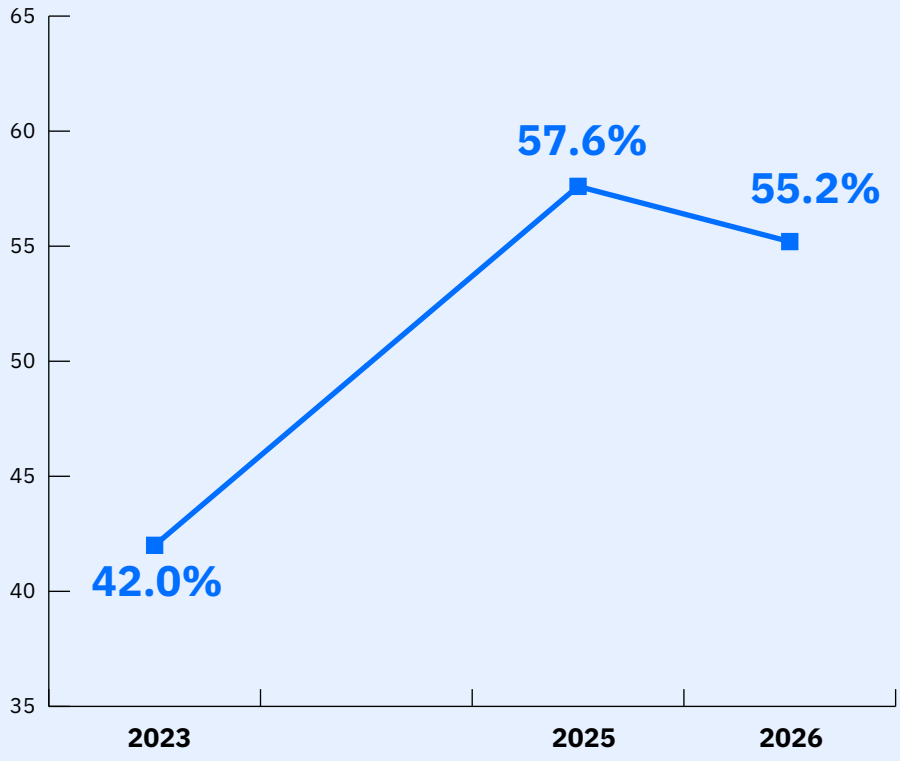
My skłaniamy się ku bardziej wyważonej interpretacji:

Regulacje skutecznie ustanowiły minimalny standard ujawniania incydentów, a utrzymujący się poziom sugeruje, że organizacje stopniowo przyswajają nowe wymagania. Jednocześnie wciąż wysoki odsetek takich przypadków pokazuje, że zmiana kultury organizacyjnej zachodzi znacznie wolniej niż zmiana przepisów. Regulacje wyznaczają minimum, ale trwała zmiana wymaga, by zgłaszanie incydentów przestało być postrzegane jako ryzykowne. A być może odwrotnie – by ukrywanie naruszeń stało się niemożliwe do usprawiedliwienia.

Wyniki badania

Specjaliści ds. bezpieczeństwa, którym polecono zachować naruszenie w tajemnicy

Źródło: Ocena stanu cyberbezpieczeństwa 2026

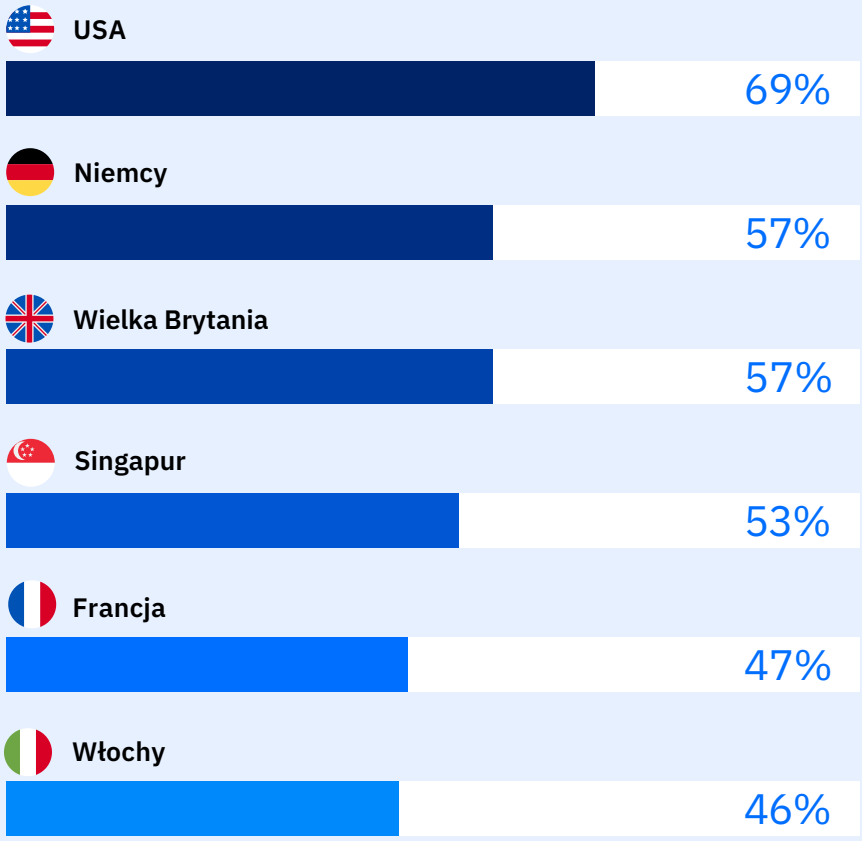


Wyniki badania

Geografia milczenia

Odsetek respondentów, którzy w ciągu ostatnich 12 miesięcy usłyszeli polecenie zachowania naruszenia bezpieczeństwa w poufności

Źródło: Ocena stanu cyberbezpieczeństwa 2026



Bilans naruszeń bezpieczeństwa

Co wydarzyło się w ciągu ostatnich 12 miesięcy? Ponad 50% organizacji deklaruje, że w ostatnim roku doświadczyło naruszenia bezpieczeństwa lub incydentu cyberbezpieczeństwa. Najczęściej były to:

41.8%
Nieautoryzowany dostęp do infrastruktury lub aplikacji chmurowych

35.9%
Atak BEC (Business Email Compromise) skutkujący stratami finansowymi lub utratą danych

25.6%
Szyfrowanie danych w celu wymuszenia okupu

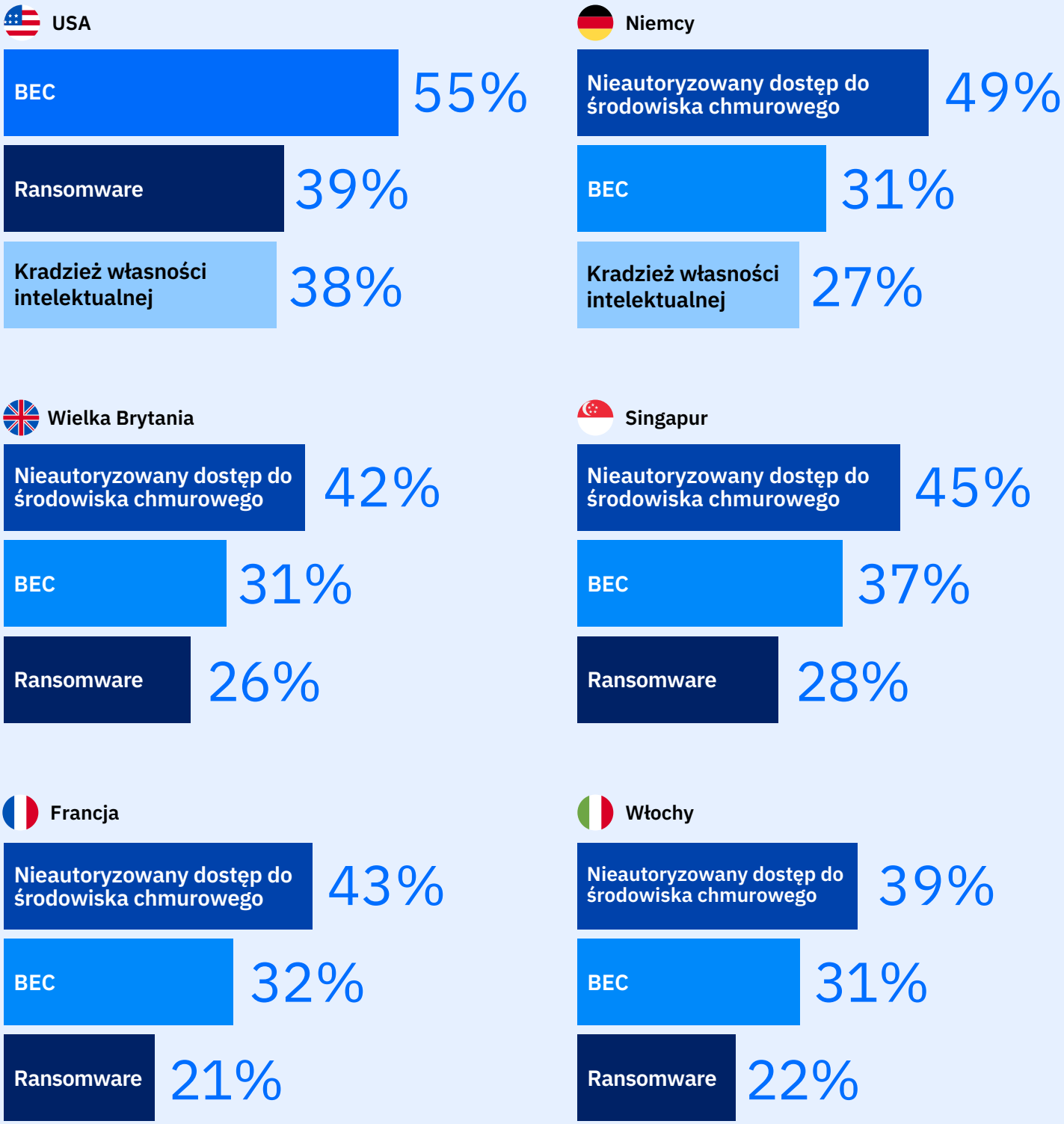
24.5%
Kradzież własności intelektualnej lub szpiegostwo przemysłowe

22.2%
Wykradanie danych w celu wymuszenia okupu

20.3%
Brak incydentów bezpieczeństwa

Jakie trzy najpoważniejsze naruszenia lub incydenty bezpieczeństwa wystąpiły w Twojej organizacji w ciągu ostatnich 12 miesięcy?

Źródło: Ocena stanu cyberbezpieczeństwa 2026



SEKCJA 2

Zagrożenia związane z AI nabierają realnych kształtów

Era AI już nadeszła – i jest uzbrojona.
Zagrożenia wykorzystujące sztuczną inteligencję oraz związane z nią ryzyko to prawdopodobnie najgorętszy temat cyberbezpieczeństwa w 2026 roku. Trzy lata temu ataki wspierane przez AI były głównie tematem konferencji. Dwa lata temu stały się rosnącym zagrożeniem. W ubiegłym roku organizacje zaczęły je zgłaszać. Dziś nasze badanie pokazuje, że cyberzagrożenia wykorzystujące AI są już potwierdzoną i powszechną rzeczywistością. Wśród licznych dyskusji o AI 53% respondentów uważa, że sztuczna inteligencja bardziej pomaga cyberprzestępcom niż obrońcom.

Co więcej, część ryzyka pochodzi z wnętrza organizacji. Wielu specjalistów IT i cyberbezpieczeństwa wskazuje, że zagrożenia są już obecne w ich środowiskach, ponieważ narzędzia AI szybko upowszechniają się w miejscu pracy. Problem polega na tym, że organizacje nie potrafią ich w pełni wykrywać ani skutecznie zabezpieczać.

52.6%

respondentów uważa, że AI bardziej pomaga atakującym niż obrońcom

> *Nie sądzę, aby wiele organizacji zadawało dziś właściwe pytania dotyczące AI. Wykorzystują liczne narzędzia wyposażone w funkcje sztucznej inteligencji, nie rozumiejąc w pełni wpływu tych możliwości na bezpieczeństwo.”*
>
> — Nicholas Jackson, Bitdefender Director of Cybersecurity Services

AI i cyberbezpieczeństwo – analiza trendów

Bitdefender wykorzystuje sztuczną inteligencję w swoich rozwiązaniach cyberbezpieczeństwa od 2008 roku i posiada dziesiątki patentów związanych z AI, dzięki czemu dysponuje bogatym doświadczeniem w budowaniu mechanizmów ochrony opartych na sztucznej inteligencji. Warto jednak zwrócić uwagę na pewien trend. W raporcie Cybersecurity Assessment 2023 nie pytaliśmy jeszcze o zagrożenia wykorzystujące AI. Sygnałów było zbyt mało, aby uzasadnić takie pytanie.

W 2024 roku już je zadaliśmy i 96% respondentów przyznało, że obawia się zagrożeń związanych ze sztuczną inteligencją.

W 2025 roku 63% stwierdziło, że ich organizacja doświadczyła ataku, który – ich zdaniem – wykorzystywał AI.

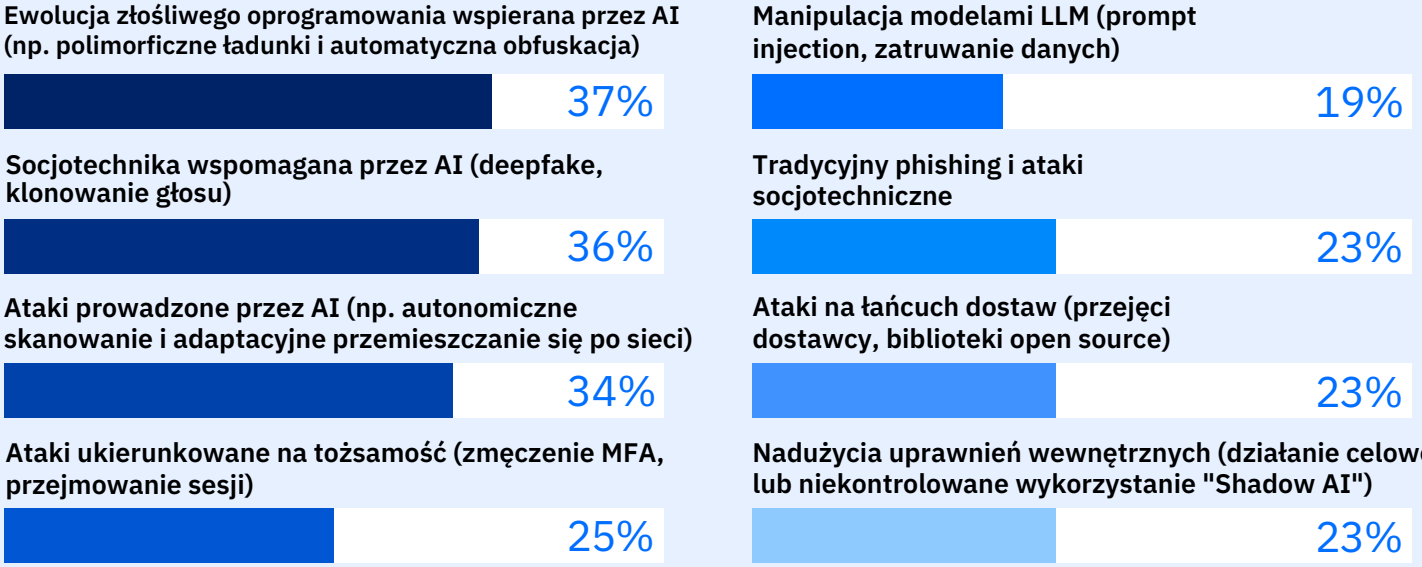
Natomiast w Raporcie Cyberbezpieczeństwa Bitdefender 2026 specjaliści IT i cyberbezpieczeństwa wskazali, że **trzy najpoważniejsze metody ataku** zagrażające ich organizacjom są bezpośrednio ***związane z wykorzystaniem sztucznej inteligencji***.

Nie ulega wątpliwości, że cyberprzestępcy coraz częściej wykorzystują AI. Laboratoria Bitdefender udokumentowały m.in. wykorzystanie modelu rozwoju opartego na AI przez grupę APT36, a nasi analitycy wykazali również, że sztuczna inteligencja pomogła innemu sprawcy przejść od prostych ataków typu script kiddie do prowadzenia kampanii ransomware. Jak dotąd jednak apokalipsa cyberataków opartych na AI, której wielu się obawiało, nie nastąpiła.

Wyniki badania

Najważniejsze metody ataku zagrażające mojej organizacji

Źródło: Ocena stanu cyberbezpieczeństwa 2026

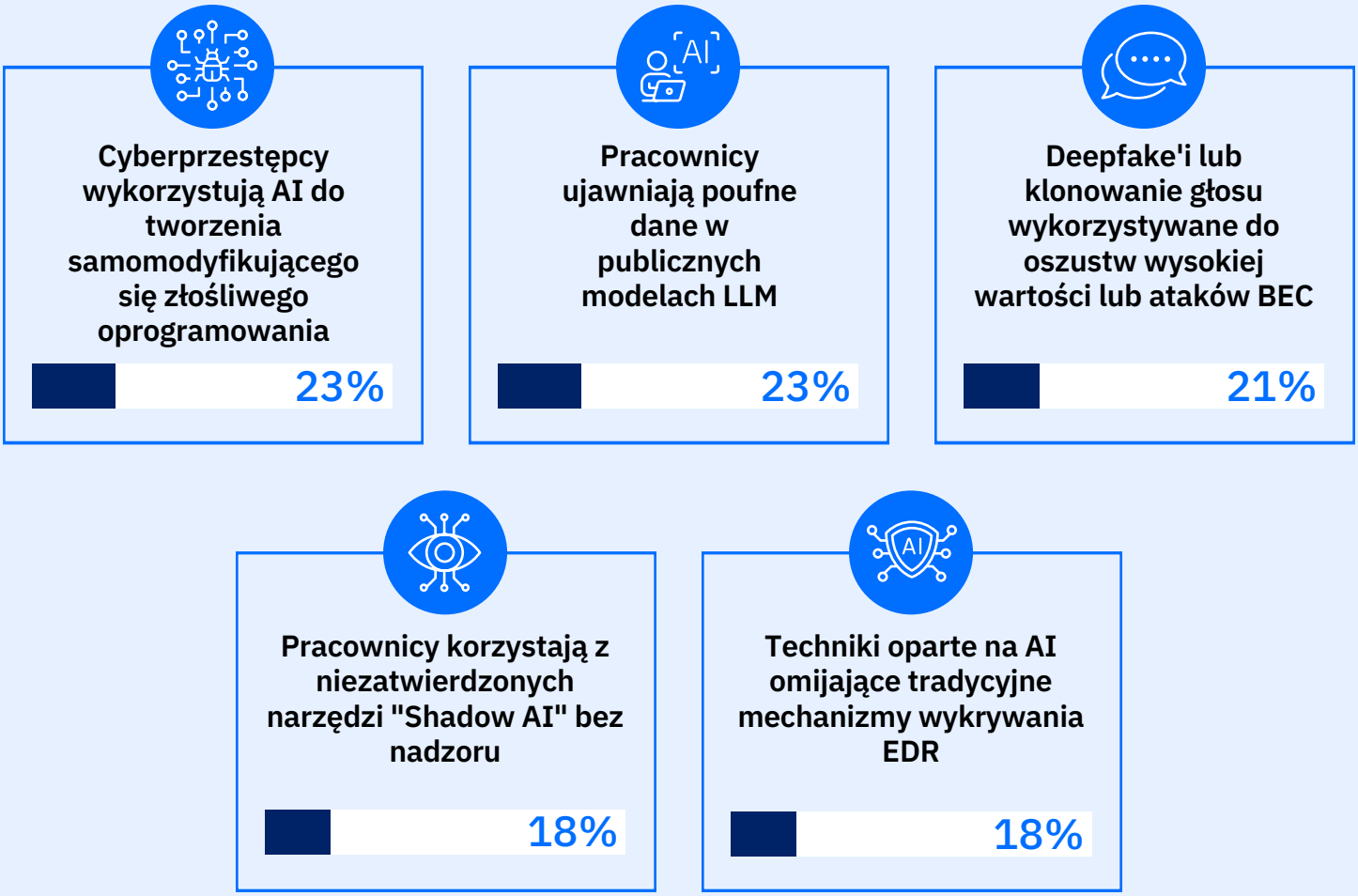


> *Największa obawa wskazana w badaniu czyli ewolucja złośliwego oprogramowania wspieranego przez AI to jednocześnie zagrożenie, które uważam za najbardziej przeceniane. Udokumentowaliśmy przypadki, w których grupa APT36 tworzyła złośliwe oprogramowanie generowane przez AI praktycznie każdego dnia. Żaden z tych przykładów nie był szczególnie innowacyjny. Zagrożenie jest realne, ale nie oznacza przełomu w rozwoju malware. AI nie podniosła jego jakości, a podniosła jedynie poziom przeciętnych ataków.”*
>
> — Bitdefender Technical Solutions Director Martin Zugec

Wyniki badania

Scenariusze AI oceniane jako „ekstremalnie ryzykowne”

Źródło: Ocena stanu cyberbezpieczeństwa 2026



Problem „Shadow AI”

Podczas gdy organizacje przygotowują się na przyszłe ataki wykorzystujące AI ze strony cyberprzestępców, wiele z nich może już dziś nie doceniać zagrożeń związanych z AI powstających we własnym środowisku. W tegorocznym badaniu jedynie 51,8% organizacji deklaruje pełną widoczność narzędzi AI wykorzystywanych przez firmę i jej pracowników.

Pozostałe działają z ograniczoną wiedzą (44,8%) lub praktycznie bez niej (2,5%).

To nie tylko problem technologiczny, ale również luka w obszarze zarządzania i nadzoru.

Shadow AI może przypominać dawne zjawisko Shadow IT, jednak jest znacznie trudniejsze do wykrycia, a ryzyko wycieku danych jest wielokrotnie większe.

Wyniki badania

Widoczność modeli LLM i narzędzi AI wykorzystywanych przez pracowników

Źródło: Ocena stanu cyberbezpieczeństwa 2026

Pełna widoczność: Monitorujemy i rejestrujemy wykorzystanie wszystkich zatwierdzonych i niezatwierdzonych narzędzi AI, w tym rozszerzeń przeglądarki oraz wywołań API.

Częściowa widoczność: Monitorujemy firmowe modele LLM, ale nie mamy pełnej wiedzy o indywidualnych subskrypcjach Shadow AI ani prywatnych kontach wykorzystywanych do celów służbowych.

Brak widoczności: Obecnie nie monitorujemy, z jakich narzędzi AI ani modeli LLM korzystają nasi pracownicy.

	Pełna widoczność	Częściowa widoczność	Brak widoczności
Francja	42%	56%	2%
Niemcy	52%	43%	4%
Włochy	50%	45%	6%
Singapur	48%	50%	2%
Wielka Brytania	58%	40%	2%
USA	63%	37%	--

Dokąd zmierza sztuczna inteligencja?

Wiemy, że sztuczna inteligencja zmienia wszystko — organizacje, zespoły bezpieczeństwa i działania cyberprzestępców. Blisko 6 na 10 specjalistów IT i cyberbezpieczeństwa (59,2%) twierdzi, że ich organizacja doświadczyła ataków socjotechnicznych, które ich zdaniem wykorzystywały AI. Ponad połowa (55,7%) deklaruje wystąpienie ataków z użyciem złośliwego oprogramowania wspieranego przez AI. Z kolei 70,1% organizacji obserwuje coraz bardziej zaawansowane kampanie phishingowe wykorzystujące sztuczną inteligencję.

Patrząc w przyszłość zagrożeń związanych z AI, niewielu respondentów uważa już, że są one „głównie medialnym szumem” (17,5%). Grono sceptyków systematycznie się kurczy. Jednocześnie nadal trudno jednoznacznie ocenić, jak daleko zajdzie rozwój tego typu zagrożeń.

Dzisiejsze wiadomości phishingowe wykorzystują treści generowane przez AI oraz poprawną lokalną gramatykę, dzięki czemu skuteczniej omijają podstawowe filtry. Ich skuteczność dorównuje legalnym kampaniom marketingowym. Skuteczna ochrona wymaga monitorowania zagrożeń również po dostarczeniu wiadomości oraz szybkiej reakcji — tradycyjne rozwiązania po prostu za tym nie nadążają.”

— Brian Byrne,
Bitdefender VP of Email Security

Grono sceptyków systematycznie się kurczy.

17.5%

specjalistów ds. bezpieczeństwa uważa dziś, że ataki wykorzystujące AI są „głównie medialnym szumem”

Wyniki badania

Techniczna nowość zagrożeń wykorzystujących AI

Źródło: Ocena stanu cyberbezpieczeństwa 2026

AI wzmacnia cały istniejący łańcuch ataku.
Przyspiesza każdy jego etap.

AI zwiększa skuteczność socjotechniki, jednak złośliwe oprogramowanie i techniki wykorzystania podatności pozostają w większości tradycyjne.

AI stanowi przełom technologiczny. Umożliwia tworzenie nowego, natywnego dla AI złośliwego oprogramowania oraz autonomicznych łańcuchów ataku.

SEKCJA 3

Luka między optymizmem a rzeczywistym poziomem cyberbezpieczeństwa

Cyberbezpieczeństwo nie jest dziedziną kojarzoną z optymizmem. Mimo to tegoroczna edycja raportu Bitdefender Cybersecurity Assessment ujawnia wyraźny trend obserwowany we wszystkich badanych krajach: kadra zarządzająca znacznie lepiej ocenia poziom cyberbezpieczeństwa niż specjaliści odpowiedzialni za jego codzienne zapewnianie.

Średnio liderzy IT i cyberbezpieczeństwa ocenili poziom bezpieczeństwa swoich organizacji oraz ich zdolność do radzenia sobie z zagrożeniami o 8% wyżej niż pracownicy pierwszej linii.

8%

średnio o tyle wyżej liderzy IT i cyberbezpieczeństwa oceniają poziom bezpieczeństwa swojej organizacji niż pracownicy pierwszej linii.

Ta różnica jest widoczna w wielu obszarach — od widoczności wykorzystania AI i wiary w możliwość eliminowania luk bezpieczeństwa, po zgodność działań z celami biznesowymi, rozwój kompetencji oraz zarządzanie zgodnością z przepisami.Podczas gdy kadra zarządzająca dostrzega postęp i realizację strategii, specjaliści pierwszej linii na co dzień mierzą się z rzeczywistością operacyjną: niedoborem personelu, zmęczeniem nadmiarem alertów, stale rosnącą powierzchnią ataku oraz coraz większą złożonością środowisk wynikającą z wykorzystania AI.

Wyniki badania za 2026 rok pokazują, że liderzy i specjaliści nie różnią się w ocenie samych zagrożeń — patrzą na nie po prostu z różnych perspektyw. W kolejnych latach zmniejszenie tej różnicy może okazać się równie ważne jak eliminowanie technicznych luk bezpieczeństwa.

Różnica w postrzeganiu między kadrą zarządzającą a specjalistami

Źródło: Ocena stanu cyberbezpieczeństwa 2026

Liderzy
IT i cyberbezpieczeństwa

Specjaliści
odpowiedzialni za wdrażanie i zarządzanie zabezpieczeniami

	Liderzy	Różnica	Specjaliści
Pełna widoczność wykorzystania AI	57.8%	11.9 punktów	45.9%
Pewność w eliminowaniu luk bezpieczeństwa	74.0%	6.9 punktów	67.1%
Zgodność działań cyberbezpieczeństwa z celami biznesowymi	72.8%	7.4 punktów	65.4%
Jasność co do kompetencji, które należy rozwijać wewnątrz organizacji	73.7%	5.0 punktów	68.7%
Przytłoczenie wymaganiami związanymi ze zgodnością z przepisami	65.2%	7.1 punktów	58.1%

SEKCJA 4

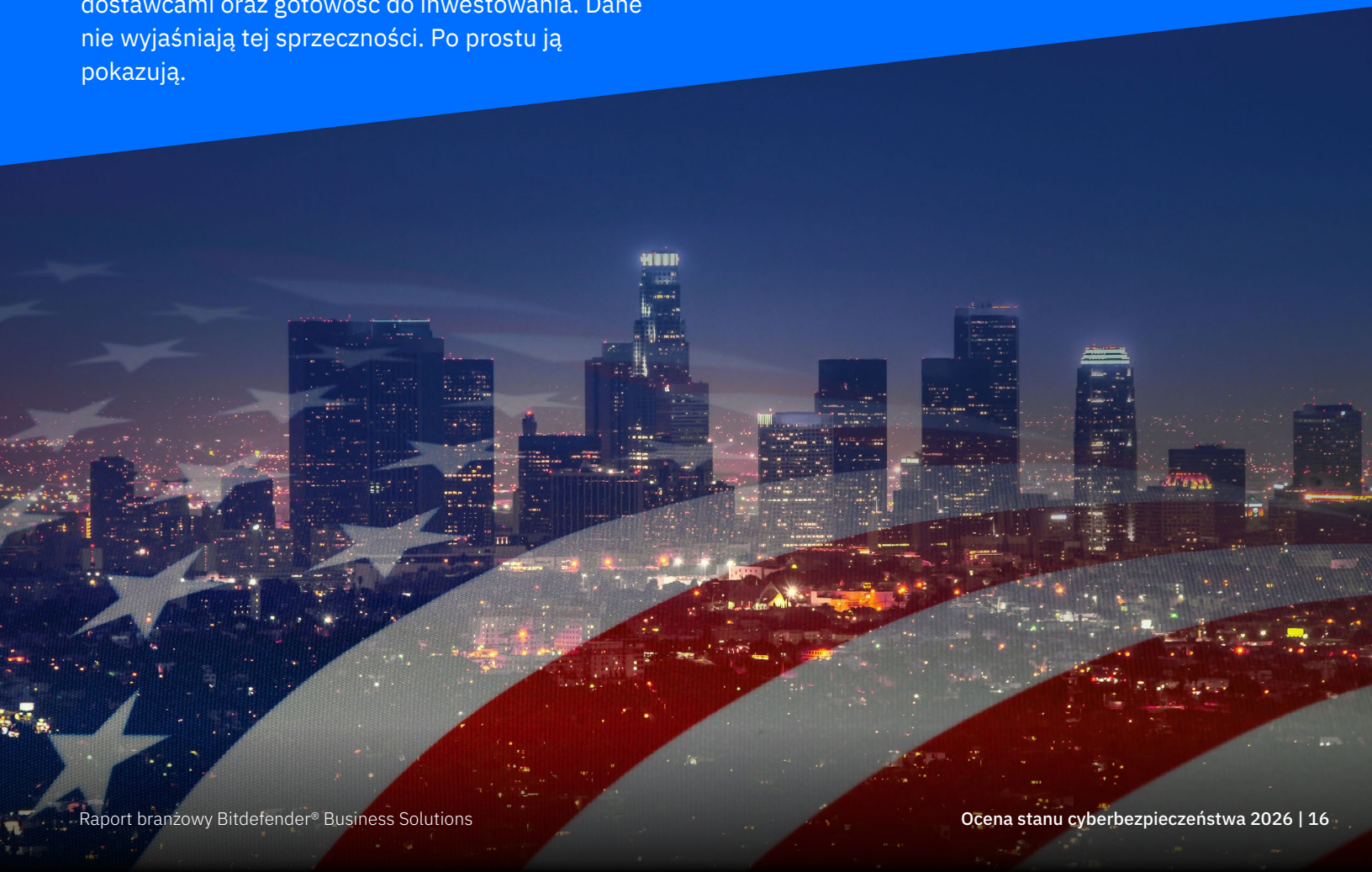
Amerykański paradoks

Nadmierna pewność siebie, niewystarczające zasoby

Respondenci ze Stanów Zjednoczonych są jednocześnie najbardziej przeciążeni i najbardziej pewni siebie spośród wszystkich uczestników badania. Częściej zgłaszają przypadki ukrywania naruszeń, większą liczbę ataków wykorzystujących AI oraz większą złożoność środowisk bezpieczeństwa. Jednocześnie wyżej oceniają poziom bezpieczeństwa swoich organizacji, relacje z dostawcami oraz gotowość do inwestowania. Dane nie wyjaśniają tej sprzeczności. Po prostu ją pokazują.

18.7%

W Stanach Zjednoczonych odsetek obchodzenia mechanizmów bezpieczeństwa jest wyższy od średniej światowej



Wskaźniki przeciążenia wśród respondentów z USA należą do najwyższych w całym badaniu. 69,7% uważa, że AI daje przewagę cyberprzestępcom (wobec 52,6% globalnie). 61,7% ma trudności z obsługą rosnącej liczby alertów (wobec 44,7%). 66,7% twierdzi, że mechanizmy bezpieczeństwa są regularnie omijane (wobec 48,0%). 63,2% deklaruje brak możliwości zapewnienia ochrony 24/7 (wobec 47,6%), co pozostaje jednym z głównych powodów rosnącego zainteresowania usługami MDR (Managed Detection and Response).

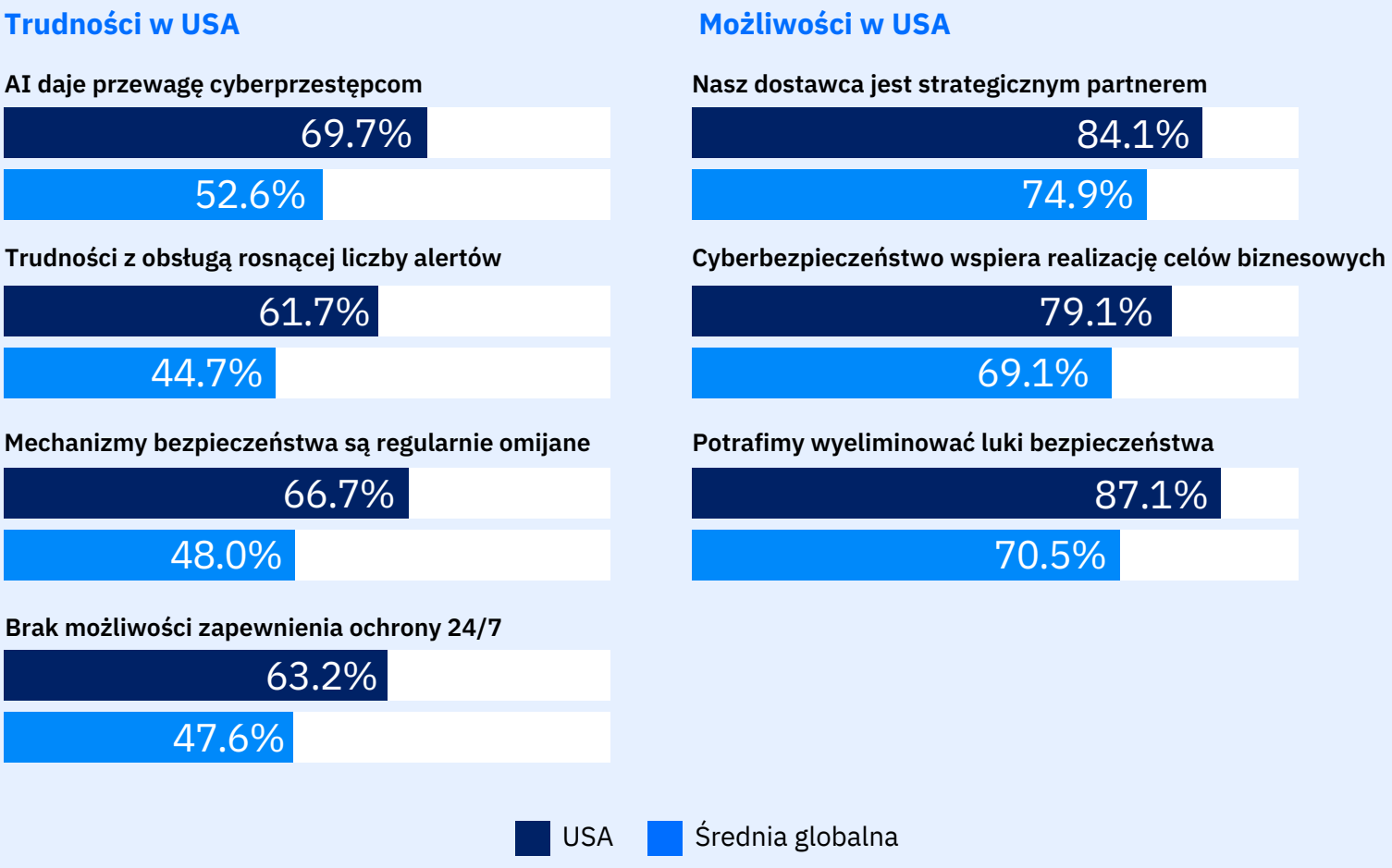
Każdy z tych wskaźników jest o 15–20 punktów procentowych wyższy od średniej światowej. To nie przypadek. To wyraźny sygnał.

Jednak gdy spojrzymy na poziom deklarowanej pewności siebie, obraz całkowicie się odwraca. 84,1% respondentów z USA postrzega swojego dostawcę jako strategicznego partnera (wobec 74,9% globalnie). 78,1% uważa, że działania z zakresu cyberbezpieczeństwa są zgodne z celami biznesowymi (wobec 69,1%). 87,1% jest przekonanych, że ich organizacja potrafi wyeliminować luki bezpieczeństwa (wobec 70,5%). Amerykańskie organizacje intensywnie inwestują w cyberbezpieczeństwo, ale jednocześnie działają pod dużą presją. Te same uwarunkowania, które sprzyjają większym inwestycjom, mogą również prowadzić do wyższej samooceny. Obie te rzeczy mogą być jednocześnie prawdziwe.

Wyniki badania

Respondenci z USA są jednocześnie najbardziej przeciążeni i najbardziej pewni siebie spośród wszystkich uczestników badania.

Źródło: Ocena stanu cyberbezpieczeństwa 2026



SEKCJA 5

Nowe pytanie już nie brzmi „gdzie?”, lecz „kto?”

Przez lata organizacje koncentrowały się na tym, gdzie przechowywane są ich dane. Dziś ważniejsze staje się pytanie, kto może mieć do nich dostęp, kto je przetwarza i czyjej jurysdykcji podlegają. Wraz ze wzrostem znaczenia niezależności danych, liderzy IT i cyberbezpieczeństwa coraz częściej uwzględniają ten aspekt przy wyborze dostawców.

76%

niezależność danych staje się coraz ważniejszym kryterium przy podejmowaniu decyzji zakupowych

Od formalności do czynnika decydującego o współpracy

Znaczenie niezależności danych rośnie we wszystkich badanych regionach, choć z różnym natężeniem. Największą gotowość do zmiany dostawcy deklarują respondenci z USA (87,1%), następnie z Wielkiej Brytanii (85,0%) oraz Niemiec (77,0%). Nawet kraje z najniższymi wynikami — Francja (62,5%) i Włochy (68,5%) — wskazują, że większość organizacji byłaby gotowa zmienić dostawcę z tego powodu.

Powody są różnorodne. Znaczenie mają zarówno wymagania regulacyjne, napięcia geopolityczne, jak i obawy związane z uzależnieniem od zagranicznych technologii.

Szczególnie interesująca jest niewielka różnica pomiędzy odsetkiem respondentów twierdzących, że niezależność danych ma znaczenie (77%), a tymi, którzy byliby gotowi zmienić z tego powodu dostawcę (76,1%). Wyniki są niemal identyczne. Oznacza to, że dla większości organizacji suwerenność danych nie jest już dodatkową wartością — stała się jednym z kluczowych kryteriów wyboru dostawcy.

Raport IDC Market Note 2026 pokazuje, jak wygląda to w praktyce.

“Pytania przestały dotyczyć wyłącznie tego, gdzie hostowana jest platforma. Dziś organizacje pytają: kto nią zarządza, z jakiego kraju oraz który zagraniczny rząd może zgodnie z prawem wywierać wpływ na dostawców naszej kluczowej technologii?”

Tego rodzaju analiza prowadzi organizacje do poszukiwania rozwiązań, które już w założeniu zapewniają bezpieczeństwo, zgodność z przepisami oraz niezależność danych.

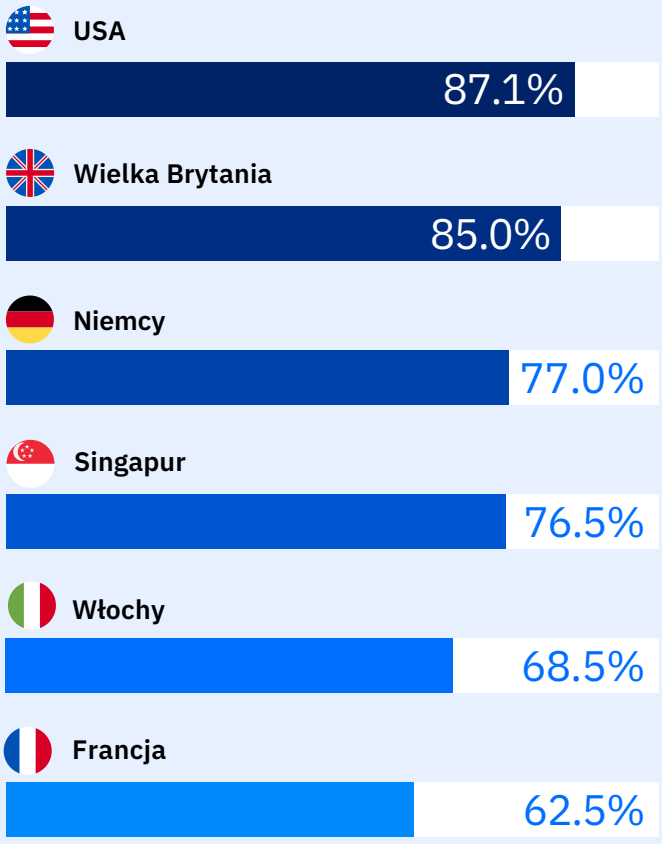
“W październiku 2025 roku OVHcloud oraz rumuńska firma Bitdefender ogłosiły uruchomienie niezależnej platformy cyberbezpieczeństwa hostowanej w usłudze OVHcloud posiadającej certyfikat SecNumCloud.” zauważa IDC[1]

[1] IDC Market Note: Bitdefender & OVHcloud Join Forces with European Sovereign Cybersecurity Platform Offering (Doc #EUR254251926, Luty 2026)

Wyniki badania

Gotowość do zmiany dostawcy ze względu na niezależność danych

Źródło: Ocena stanu cyberbezpieczeństwa 2026



Wniosek
Przeanalizuj umowy z dostawcami pod kątem miejsca przechowywania danych, jurysdykcji oraz zapisów dotyczących podwykonawców przetwarzających dane. Jeśli dostawca nie potrafi udzielić jednoznacznych odpowiedzi, warto rozważyć współpracę z takim, który zapewnia pełną przejrzystość.

SEKCJA 6

Zagubieni w blasku sztucznej inteligencji

Laboratoria Bitdefender przeanalizowały ponad 700 000 incydentów cyberbezpieczeństwa i ustaliły, że 84% poważnych ataków wykorzystuje techniki Living off the Land (LOTL). Mimo to jedynie 20,5% respondentów wskazuje LOTL jako jedno z trzech najpoważniejszych zagrożeń. Różnica wynosząca 63,5 punktu procentowego pomiędzy rzeczywistą skalą występowania a postrzeganym znaczeniem LOTL jest największą rozbieżnością ujawnioną w tegorocznym raporcie.

84%

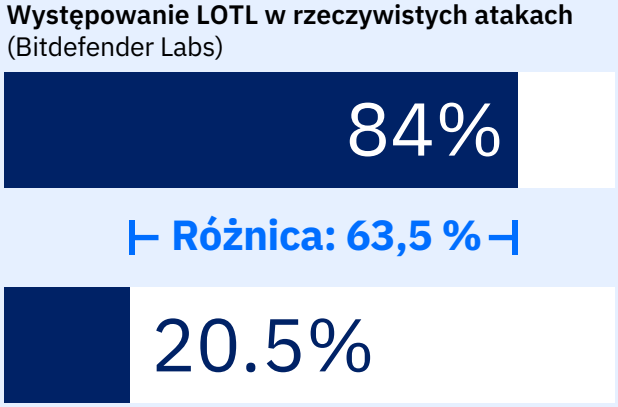
poważnych ataków wykorzystuje techniki Living off the Land (LOTL)

Problem 84% vs 20%

Czego faktycznie używają atakujący vs czym martwią się obrońcy

Źródło: Ocena stanu cyberbezpieczeństwa 2026

Wniosek
Inwestuj w architekturę bezpieczeństwa opartą przede wszystkim na zapobieganiu, która wykrywa szkodliwe wzorce zachowania niezależnie od wykorzystywanych narzędzi. Ataki LOTL z założenia omijają ochronę opartą wyłącznie na sygnaturach.



Ataki Living off the Land (LOTL) wykorzystują narzędzia już obecne w środowisku ofiary, takie jak PowerShell, WMI, RDP oraz inne legalne narzędzia administracyjne. Nie generują klasycznych sygnatur malware, ponieważ same nie są złośliwym oprogramowaniem. Działania cyberprzestępców wyglądają jak normalna aktywność administratorów, ponieważ wykorzystują te same narzędzia.

To wskazuje na długoterminowy problem bezpieczeństwa, który coraz więcej organizacji próbuje rozwiązywać poprzez ochronę opartą na zapobieganiu — taką, która zatrzymuje ataki nawet wtedy, gdy wyglądają jak standardowa aktywność.

W tegorocznym badaniu największe obawy wzbudziła ewolucja złośliwego oprogramowania wspierana przez AI (37,5%) oraz socjotechnika wspierana przez AI (36,2%). Branża ma powody, aby obawiać się zagrożeń związanych z AI, jednak narracja wokół sztucznej inteligencji przesłania uwagę od technik, które cyberprzestępcy wykorzystują najczęściej. To cyberbezpieczeństwowy odpowiednik martwienia się o rekiny podczas pływania w rzece pełnej hipopotamów.

> *Od lat rozmowa o bezpieczeństwie koncentruje się wokół wykrywania i reagowania. Nadal są to kluczowe możliwości. Nasz zespół zadał jednak pytanie: co jeśli przestaniemy dawać atakującym przestrzeń do działania już na samym początku? To prosta i fundamentalna idea, która doprowadziła nas do stworzenia rozwiązania zaprojektowanego nie tylko do reagowania na zagrożenia, ale także do zmniejszania prawdopodobieństwa ich wystąpienia.”*
>
> — Daniel Daraban,
> Bitdefender Vice President of Products

Cena złożoności

Niewidoczny problem LOTL jest częściowo objawem większego wyzwania: złożoności narzędzi. Tylko 39% respondentów określa swoje obecne rozwiązanie EDR/XDR jako „dobrze zbalansowane”. Jednocześnie pełne 40% twierdzi, że ich EDR/XDR jest tak złożone, że „wymaga znacznego ręcznego nakładu pracy” lub „nie może zostać w pełni wdrożone”.

Wyniki badania

Jak oceniamy obecnie używaną platformę EDR/XDR

Źródło: Ocena stanu cyberbezpieczeństwa 2026

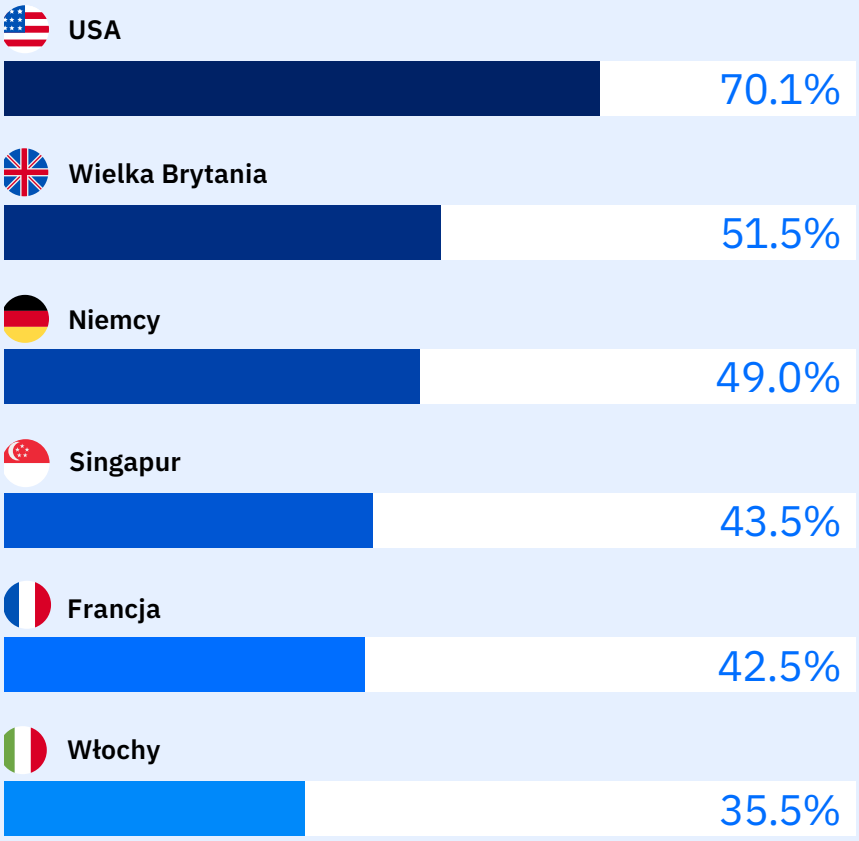
Dla niewielkich zespołów bezpieczeństwa rozwiązaniem nie jest dodawanie kolejnego pojedynczego narzędzia. Kluczowe jest konsolidowanie środowiska do mniejszej liczby lepiej zintegrowanych rozwiązań, które obejmują pełne spektrum systemów operacyjnych z jednej konsoli oraz wykorzystują AI do aktywnego ograniczania liczby luk możliwych do wykorzystania przez atakujących.

Powierzchnia ataku jest jednocześnie złożona i stale rośnie. 57,0% respondentów zgadza się, że ich organizacja musi ograniczyć powierzchnię ataku. Chcą to osiągnąć poprzez wyłączanie niepotrzebnych lub ryzykownych narzędzi, ale jednocześnie obawiają się, że może to zakłócić działanie biznesu.

Wyniki badania

“Mamy trudności z pogodzeniem ograniczeń bezpieczeństwa z produktywnością pracowników.”

Źródło: Ocena stanu cyberbezpieczeństwa 2026



Ogółem 38,0% wskazuje, że duży nakład pracy związany z utrzymywaniem reguł hardeningu i wyjątków utrudnia zmniejszenie powierzchni ataku. 34,6% jako przeszkodę wskazuje ograniczone zasoby, a 33,8% uważa, że problemem są braki w widoczności środowiska.

Rezultatem jest środowisko, w którym organizacje wiedzą, że mają zbyt wiele narzędzi i powinny je ograniczyć, ale jednocześnie nie potrafią skutecznie przełożyć tej wiedzy na działanie.

57.0%

respondentów zgadza się, że należy ograniczyć powierzchnię ataku, ale

38.0%

twierdzi, że wysokie koszty utrzymania reguł hardeningu i wyjątków utrudniają jej zmniejszenie.

SEKCJA 7

Gdy zgodność z przepisami staje się celem samym w sobie

Jeśli 56% respondentów opisuje działania związane ze zgodnością jako „głównie odhaczanie pól”, warto zapytać, co faktycznie organizacje otrzymują w zamian za ponoszone koszty. Prawdziwym miernikiem poziomu bezpieczeństwa nie jest to, czy organizacja przechodzi audyty. Jest nim to, czy potrafi zatrzymać ataki.Niezależne testy skuteczności, a nie same certyfikaty zgodności, pokazują rzeczywisty poziom ochrony.

56%

respondentów uważa, że działania związane ze zgodnością to głównie „odhaczanie pól”

Paradoks „odhaczania pól”

Dane dotyczące zgodności z raportu Bitdefender Cybersecurity Assessment 2026 tworzą paradoks, który powinien zaniepokoić każdego odpowiedzialnego za budżety audytowe.

Większość (62%) specjalistów IT i cyberbezpieczeństwa twierdzi, że utrzymanie zgodności jest przytłaczające. 61% uważa, że proces jest bardziej skomplikowany, niż powinien, głównie ze względu na ręczne wyszukiwanie informacji i dokumentowanie. A 56% opisuje swoje działania jako przede wszystkim oparte na spełnianiu formalnych wymagań. Te dane pokazują branżę, która przeznacza ogromne zasoby na zgodność, ale uzyskuje z tego ograniczoną wartość bezpieczeństwa.

Korelacja z obchodzeniem zabezpieczeń budzi niepokój. 48,0% wszystkich respondentów twierdzi, że mechanizmy bezpieczeństwa są regularnie, choć czasowo, omijane ze względów biznesowych. W USA odsetek ten wynosi 66,7%.

Rozwiązaniem nie jest więcej zgodności. Rozwiązaniem jest budowanie poziomu cyberbezpieczeństwa mierzonego przez niezależne testy zewnętrzne, które oceniają rzeczywistą zdolność zapobiegania atakom wykorzystującym realne techniki cyberprzestępców — a nie tylko istnienie dokumentów i procedur. Małe i średnie zespoły coraz częściej korzystają również z narzędzi do zarządzania zgodnością, aby uprościć procesy, automatyzować śledzenie wymagań i przygotowanie do audytów.

62%

specjalistów IT i cyberbezpieczeństwa uważa, że zgodność z przepisami jest przytłaczająca

56%

opisuje działania jako głównie „odhaczanie pól”

48%

zgłasza regularne obchodzenie zabezpieczeń

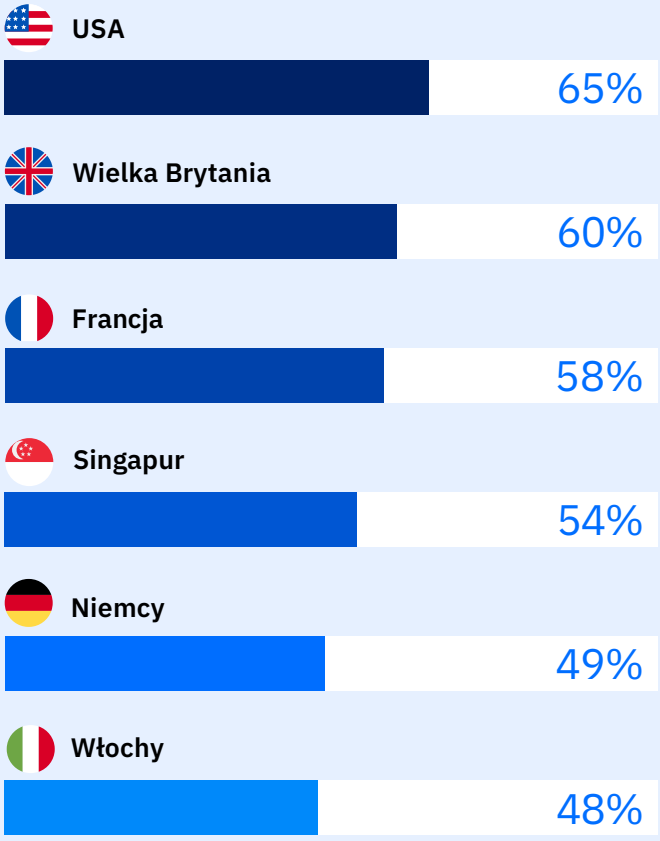
66.7%

respondentów z USA twierdzi, że mechanizmy bezpieczeństwa są regularnie omijane — o 18,7 punktu procentowego więcej niż średnia globalna

Wyniki badania

Strategia bezpieczeństwa napędzana zgodnością formalną zamiast rzeczywistym zapobieganiem zagrożeniom

Źródło: Ocena stanu cyberbezpieczeństwa 2026



Wniosek
Rozważ platformy cyberbezpieczeństwa z wbudowanym monitoringiem zgodności, które upraszczają zbieranie dowodów, automatyzują śledzenie wymagań i usprawniają procesy, zapewniając gotowość do audytów.

SEKCJA 8

Wpływ luki kompetencyjnej i analiza jej przyczyn

Kryzys kompetencji w cyberbezpieczeństwie nie jest nowym zjawiskiem.
Tegoroczne badanie pokazuje jednak, że specjaliści IT i cyberbezpieczeństwa wskazują wiele różnych przyczyn niedoboru kompetencji w swoich organizacjach.

48%

twierdzi, że nie jest w stanie zapewnić ochrony 24/7

Wyniki badania

Główna przyczyna niedoboru kompetencji w mojej organizacji

Źródło: Ocena stanu cyberbezpieczeństwa 2026

Choć specjaliści IT i cyberbezpieczeństwa wskazują wiele przyczyn niedoboru kompetencji, kierownictwo coraz częściej sięga po rozwiązania, których sam proces rekrutacji nie jest w stanie zapewnić.

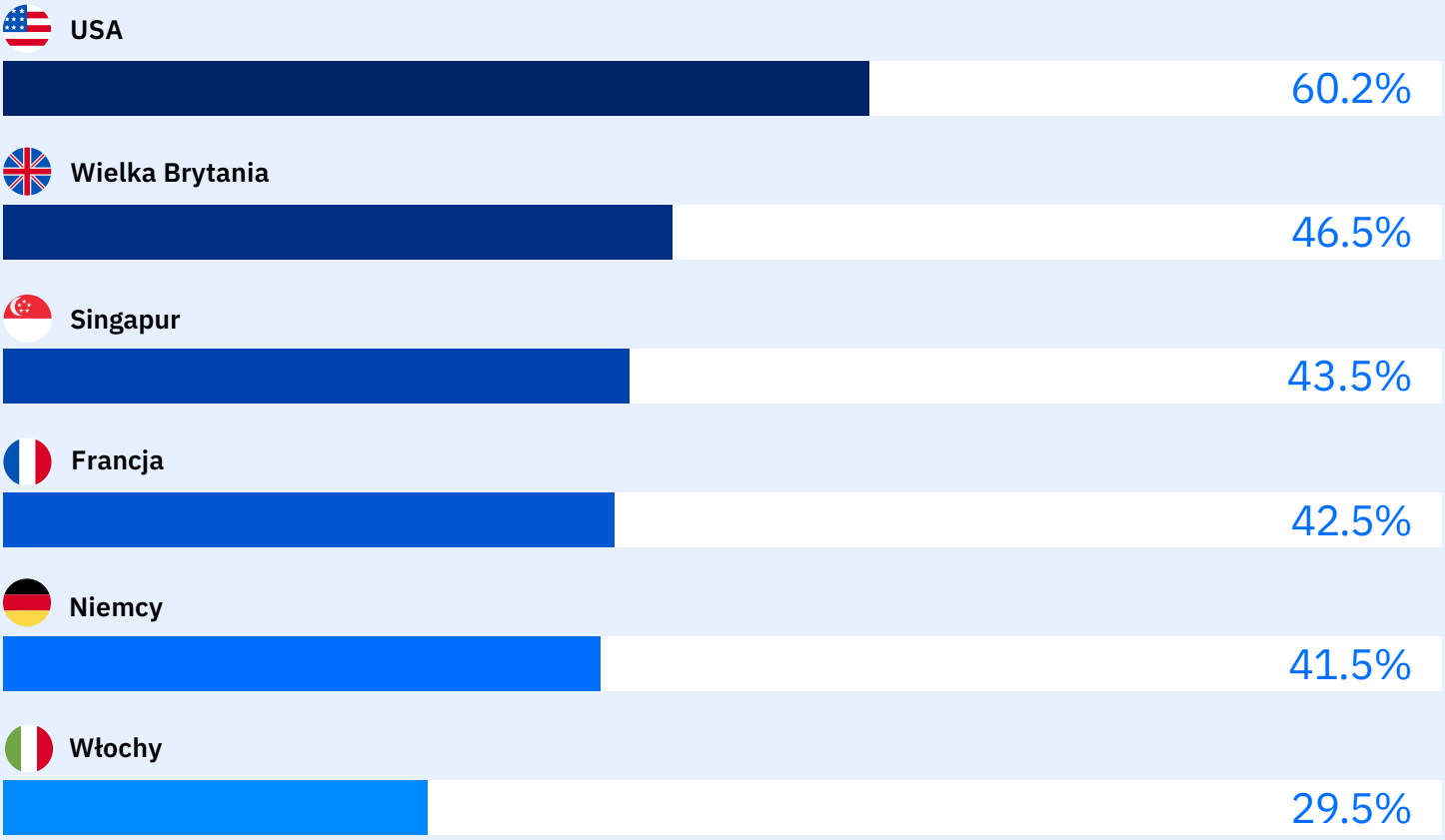
Coraz częściej oznacza to działania w dwóch obszarach: konsolidację platform bezpieczeństwa oraz wdrażanie usług MDR (Managed Detection and Response) zapewniających ochronę przez całą dobę.

Niewielkie zespoły wybierają mniejszą liczbę lepiej zintegrowanych narzędzi, obsługujących wszystkie systemy operacyjne z jednej konsoli, zamiast kolejnych rozwiązań wymagających dodatkowych specjalistów i czasu na ich utrzymanie. Znaczna część dostępnych technologii pozostaje niewykorzystana. Najczęściej z powodu braku czasu i odpowiednich kompetencji.

Wyniki badania

Brakuje nam czasu lub wiedzy, aby w pełni wykorzystać obecnie posiadane narzędzia bezpieczeństwa

Źródło: Ocena stanu cyberbezpieczeństwa 2026



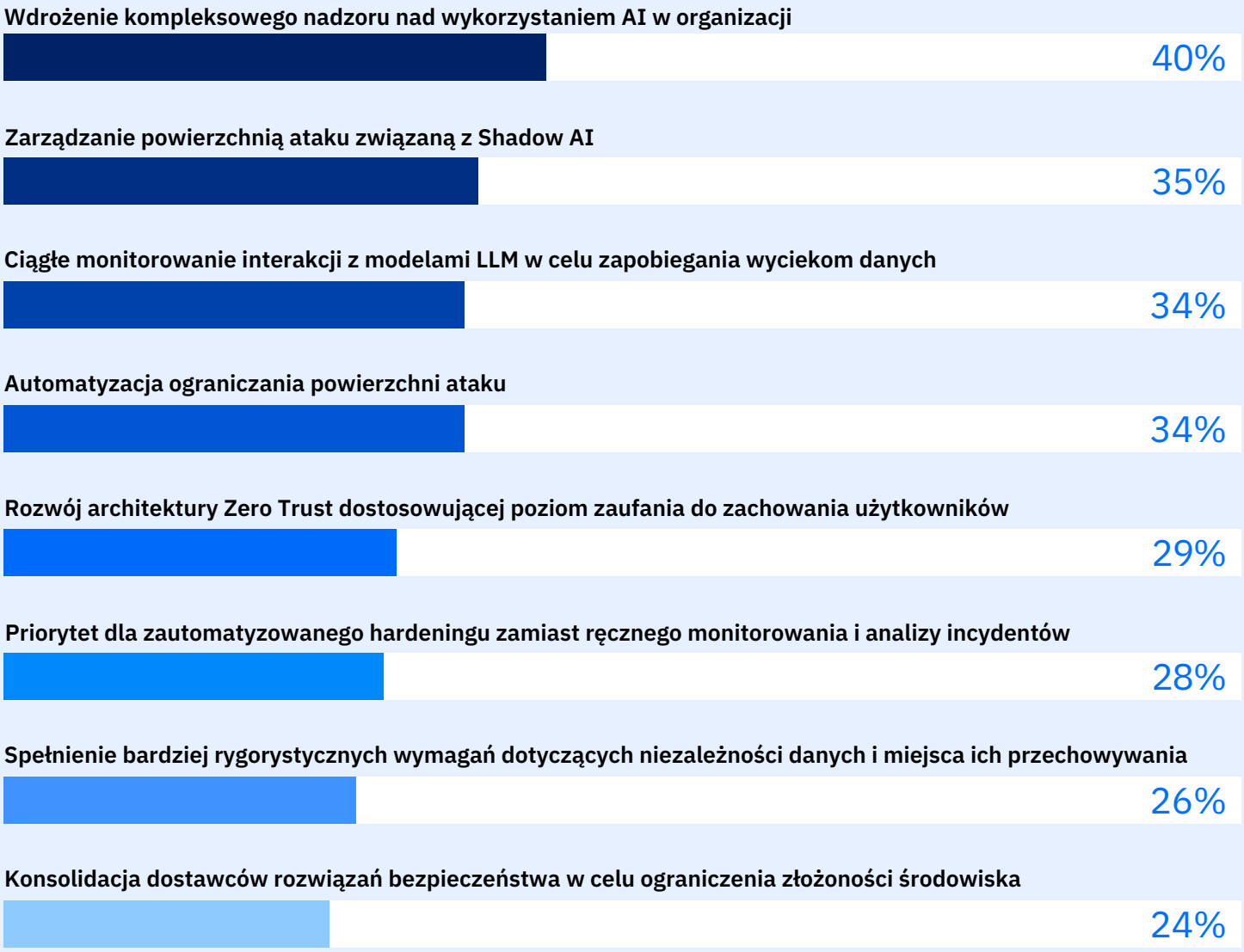
Perspektywa na przyszłość: najważniejsze inicjatywy

Zapytani o najważniejsze inicjatywy na najbliższe 12 miesięcy, respondenci najczęściej wskazywali projekty związane ze sztuczną inteligencją, co potwierdza rosnące znaczenie zagrożeń opisanych w tym raporcie.

Wyniki badania

Trzy najważniejsze inicjatywy z zakresu cyberbezpieczeństwa w ciągu najbliższych 12 miesięcy

Źródło: Ocena stanu cyberbezpieczeństwa 2026



PODSUMOWANIE

Spojrzenie w przyszłość

Branża cyberbezpieczeństwa nie stoi w miejscu. Organizacje inwestują więcej, szybciej modernizują swoje środowiska, konsolidują narzędzia, wdrażają sztuczną inteligencję oraz coraz większy nacisk kładą na odporność cyfrową, niezależność danych i efektywność operacyjną. Pod wieloma względami wyniki tego raportu pokazują branżę, która aktywnie dostosowuje się do dynamicznie zmieniających się zagrożeń.

Jednocześnie dane ujawniają głębsze napięcia. Złożoność środowisk rośnie szybciej niż ich upraszczanie. Zgodność z przepisami zbyt często przesłania działania zapobiegawcze. Sztuczna inteligencja zmienia zarówno metody ataku, jak i obrony. Przez cały raport powraca również jeden motyw — różnica pomiędzy postrzeganiem zagrożeń a rzeczywistością operacyjną. Liderzy i specjaliści inaczej oceniają ryzyko. Organizacje rozpoznają większość zagrożeń, ale często mają trudności z właściwym ustaleniem priorytetów wobec tych, które powodują największe szkody.

Organizacje najlepiej przygotowane na przyszłość niekoniecznie będą dysponowały największym budżetem lub największą liczbą narzędzi. Będą to organizacje, które ograniczą złożoność, zmniejszą powierzchnię ataku, dostosują działania z zakresu cyberbezpieczeństwa do realiów operacyjnych i będą konsekwentnie koncentrować się na rzeczywistych efektach, a nie na pozorach bezpieczeństwa.

Największym wyzwaniem nie będzie wyłącznie obrona przed zagrożeniami jutra. Będzie nim budowanie programów cyberbezpieczeństwa zdolnych do ciągłego dostosowywania się do zmian bez utraty tego, co pozostaje najważniejsze, czyli solidnych fundamentów bezpieczeństwa.

O Bitdefender

Bitdefender to zaufanie potwierdzone w praktyce.

Miliony użytkowników indywidualnych, firm i instytucji publicznych na całym świecie powierzają Bitdefender ochronę swoich środowisk cyfrowych przed najbardziej zaawansowanymi cyberzagrożeniami.

Skuteczność Bitdefender potwierdzają również niezależne testy branżowe. W latach 2013–2024 firma zdobyła pięć tytułów „Product of the Year" przyznawanych przez AV-Comparatives — osiągnięcie, którego nie powtórzył żaden inny oceniany producent. Bitdefender został również dwukrotnie wyróżniony przez Gartner® jako: Visionary w raporcie 2026 Gartner Magic Quadrant™ for Endpoint Protection Platforms oraz Customers' Choice w Gartner Peer Insights™ Voice of the Customer for Endpoint Protection Platforms

Firma jest także regularnie wyróżniana w raportach IDC.

Zintegrowana platforma bezpieczeństwa Bitdefender łączy: zaawansowaną analizę zagrożeń, ochronę wykorzystującą AI, ograniczanie powierzchni ataku, XDR (Extended Detection and Response), MDR (Managed Detection and Response), tworząc jeden spójny ekosystem bezpieczeństwa, który upraszcza zarządzanie cyberbezpieczeństwem i zwiększa odporność organizacji.

Dzięki wieloletniemu doświadczeniu, setkom patentów oraz jednemu z najbardziej cenionych na świecie zespołów badawczych ds. cyberbezpieczeństwa, Bitdefender pomaga organizacjom ograniczać złożoność, wzmacniać ochronę i budować odporność cyfrową w świecie stale ewoluujących zagrożeń.

Więcej informacji:
https://bitdefender.pl/antywirus-dla-firm/

"Rosnąca powierzchnia ataku, dynamiczny wzrost zagrożeń wykorzystujących AI oraz utrzymująca się presja operacyjna zmuszają organizacje do całkowitego przemyślenia podejścia do cyberbezpieczeństwa. Wyniki tego raportu jasno pokazują, że nowoczesne strategie bezpieczeństwa muszą wykraczać poza reaktywne mechanizmy ochrony. Powinny stale ograniczać ryzyko, zapewniać właściwy nadzór nad wykorzystaniem AI oraz wspierać zgodność z przepisami w środowisku, w którym cyberprzestępcy działają szybciej, skuteczniej i coraz częściej wykorzystują automatyzację."

— Andrei Florescu
President and General Manager of
Bitdefender Business Solutions Group

Dlaczego miliony użytkowników ufają Bitdefender

Bitdefender chroni miliony użytkowników w ponad 170 krajach, łącząc wieloletnie doświadczenie w cyberbezpieczeństwie z innowacjami opartymi na AI oraz ścisłą współpracą z organami ścigania na całym świecie.

50mld+

zagrożeń blokowanych każdego roku

$1.6mld USD+

udaremnionych płatności okupów

15+ lat

innowacji w zakresie bezpieczeństwa opartego na AI

30+

bezpłatnych narzędzi do odszyfrowywania ransomware udostępnionych publicznie

580+

zgłoszonych patentów, w tym przełomowych rozwiązań z obszaru uczenia maszynowego i wykrywania zaawansowanych zagrożeń

30+

partnerstw z organami ścigania na całym świecie wspierających walkę z ransomware

50%+

pracowników Bitdefender zajmuje się badaniami i rozwojem

Bitdefender

Bitdefender jest światowym liderem cyberbezpieczeństwa, dostarczającym rozwiązania klasy premium w zakresie zapobiegania zagrożeniom, ich wykrywania i reagowania. Chroniąc miliony środowisk użytkowników indywidualnych, przedsiębiorstw i instytucji publicznych, Bitdefender należy do najbardziej zaufanych ekspertów w dziedzinie eliminowania zagrożeń, ochrony prywatności, tożsamości cyfrowej oraz danych, a także budowania odporności cyfrowej. Dzięki znaczącym inwestycjom w badania i rozwój laboratoria Bitdefender wykrywają setki nowych zagrożeń w każdej minucie i każdego dnia analizują miliardy zapytań dotyczących zagrożeń. Firma jest pionierem innowacji w obszarach ochrony przed malware, bezpieczeństwa IoT, analizy behawioralnej oraz sztucznej inteligencji. Technologie Bitdefender są wykorzystywane przez ponad 180 najbardziej rozpoznawalnych marek technologicznych na świecie. Założona w 2001 roku firma obsługuje klientów w ponad 170 krajach i posiada biura na całym świecie. Więcej informacji: **bitdefender.pl**

Trusted. Always.

Metodologia i zastrzeżenia

Badanie oraz analiza zostały przeprowadzone w okresie od kwietnia do czerwca 2026 roku. Objęły 1 200 specjalistów IT i cyberbezpieczeństwa z sześciu krajów: Francji, Niemiec, Włoch, Singapuru, Wielkiej Brytanii oraz Stanów Zjednoczonych. Respondentami byli przedstawiciele kadry kierowniczej (od menedżerów średniego szczebla po najwyższe kierownictwo) oraz specjaliści odpowiedzialni za codzienne działania z zakresu cyberbezpieczeństwa.

Wnioski, statystyki i rezultaty przedstawione w raporcie odzwierciedlają opinie, doświadczenia i postrzeganie respondentów w momencie prowadzenia badania. Nie stanowią one potwierdzonych faktów dotyczących konkretnych organizacji, produktów ani usług, ani nie są audytowanymi, zweryfikowanymi lub niezależnie potwierdzonymi danymi dotyczącymi rzeczywistych incydentów bezpieczeństwa, ujawniania naruszeń czy praktyk związanych ze zgodnością z przepisami.

Wszystkie odpowiedzi zostały zebrane anonimowo. Na podstawie prezentowanych danych nie można zidentyfikować żadnego respondenta ani reprezentowanej przez niego organizacji. Zbiorcze wyniki mają wyłącznie charakter informacyjny i edukacyjny. Nie należy ich traktować jako porady prawnej, regulacyjnej ani profesjonalnej.

Bitdefender nie udziela żadnych wyraźnych ani dorozumianych gwarancji dotyczących dokładności, kompletności lub wiarygodności informacji zawartych w niniejszym raporcie. Przed podjęciem decyzji na podstawie przedstawionych informacji zaleca się przeprowadzenie własnej analizy oraz konsultację z odpowiednimi specjalistami.

Odniesienia do materiałów stron trzecich, w tym raportów analitycznych, publikacji branżowych i badań zewnętrznych, zostały zamieszczone wyłącznie w celach informacyjnych i nie oznaczają poparcia ani współpracy z wymienionymi podmiotami, o ile nie wskazano tego wyraźnie.

Bitdefender

BONUS DLA CZYTELNIKÓW

Oszczędź nawet

150 PLN

KOD RABATOWY
RAPORT2026

kod rabatowy do użycia w koszyku
na produkty Total Security, Family Pack
oraz Mobile Security for Android & iOS

bitdefender.pl