CLOUDFLARE

2026

Cloudflare Security Signals Report

Odporność autonomiczna

PRZEDMOWA MICHELLE ZATLYN

Wszystko się zmienia.

Sztuczna inteligencja przechodzi z fazy pilotażowej do fazy produkcyjnej, systemy autonomiczne przyspieszają podejmowanie decyzji, a gospodarka cyfrowa ewoluuje w czasie rzeczywistym. Dla liderów gotowych do działania takie tempo zmian stwarza realne możliwości.

Odporność stała się nową przewagą konkurencyjną. W miarę jak systemy inteligentne przekształcają gospodarkę cyfrową, liderzy mogą projektować mechanizmy ochronne przewidujące zmiany, tworzyć systemy zdolne do adaptacji oraz obracać zmienność w przewagę.

Cloudflare zarządza jedną z największych na świecie sieci globalnych, która obejmuje ponad 330 miast w przeszło 120 krajach. Chronimy miliony podmiotów internetowych, powstrzymujemy ponad 230 mld cyberataków każdego dnia i obsługujemy 2,5 mld żądań botów dziennie. Z tej perspektywy dostrzegamy zarówno zagrożenia, jak i możliwości kształtujące Internet.

Publikacja ***2026 Cloudflare Security Signals Report*** zawiera praktyczne wnioski, których liderzy potrzebują już dziś, jak również pokazuje siły przekształcające krajobraz cyfrowy, aby umożliwić skuteczne zarządzanie systemami inteligentnymi, bezpieczną modernizację oraz budowanie odporności od podstaw.

Naszą misją jest pomoc w budowaniu lepszego Internetu. W 2026 roku będzie to oznaczać pomoc w bezpiecznym i pewnym działaniu — z szybkością maszyn.

Michelle Zatlyn
Współzałożycielka, prezes
i współprzewodnicząca, Cloudflare

STRESZCZENIE

W przypadku dzisiejszych, silnie połączonych i zautomatyzowanych przedsiębiorstw model „przetrwać wstrząsy i odzyskać sprawność” już się nie sprawdza.

Takie podejście opiera się na naiwnym założeniu, że jesteśmy w stanie trafnie przewidzieć i przygotować się na każde konkretne zakłócenie. Systemy SI działają autonomicznie, platformy chmurowe koncentrują kluczowe obciążenia, a łańcuchy dostaw sięgają głęboko w nieprzejrzyste ekosystemy. W tej nowej rzeczywistości liderzy ds. bezpieczeństwa potrzebują **odporności autonomicznej, tj. systemów, które nie tylko wytrzymują presję, ale także regulują się, adaptują i odzyskują sprawność w czasie rzeczywistym**.

Choć jednak wiele organizacji sprawia wrażenie dojrzałych, nowoczesnych i dobrze zarządzanych, odporność autonomiczna nie jest widoczna w stanie równowagi. To rezultat przywództwa, który ujawnia się dopiero pod długotrwałą i silną presją.

Niniejszy raport opiera się na prostym założeniu: największe ryzyka, z jakimi przedsiębiorstwa będą mierzyć się w 2026 roku, nie wynikają z oczywistych słabości. Pojawiają się w ukrytych liniach podziału, tj. w obszarach, które podczas normalnego funkcjonowania wydają się stabilne, ale pękają, gdy rośnie tempo, skala lub poziom zakłóceń.

W tych rozdziałach przedstawiamy kadrze kierowniczej plan działania, który pozwoli wykryć te linie podziału, zanim dojdzie do ich pęknięcia. Każda sekcja zawiera konkretne pytania, które mają pobudzać wewnętrzną debatę i ujawniać ukrytą kruchość wewnątrz własnych organizacji. W erze inteligencji, autonomii i szybkości sukces należy do liderów, którzy projektują swoje organizacje tak, by potrafiły wykrywać sygnały, adaptować się i samoczynnie korygować pod presją, jednocześnie chroniąc kluczowe rezultaty w zmieniających się warunkach.

Sześć najważniejszych linii podziału

Te linie podziału nie są odosobnione. Presja w jednym obszarze może potęgować słabość w innych.

Okiełznanie algorytmu: zarządzanie SI na dużą skalę 1

Programy SI często sprawiają wrażenie uporządkowanych, nadzorowanych i opartych na jasno określonych wartościach. A jednak przy bliższej analizie wielu liderów nie potrafi jasno wyjaśnić, gdzie działa SI, jakich danych dotyka ani kto ponosi odpowiedzialność, gdy wyniki okazują się błędne. Widoczne na pierwszy rzut oka postępy często maskują lukę w zakresie widoczności i odpowiedzialności, która ujawnia się dopiero wtedy, gdy presję wywierają regulatorzy, klienci lub incydenty.

Zaufanie w erze szybkości maszyn: projektowanie autonomii 2

Systemy autonomiczne działają dobrze, gdy warunki są przewidywalne. Pod presją decyzje zapadają szybciej, niż nadąża ludzki nadzór, a zaufanie jest zakładane, zamiast być projektowane. Ta linia podziału pokazuje, czy delegowanie było świadome, czy też kompetencje po cichu przesunęły się w stronę maszyn, bez wyraźnych granic, odpowiedzialności i kontroli w czasie rzeczywistym.

Ukryte łańcuchy dostaw: ujawnianie niewidocznych zależności 3

Przedsiębiorstwa sprawiają wrażenie zdywersyfikowanych i bogatych w partnerów, ale są uzależnione od warstw usług stron trzecich i czwartych, których w pełni nie dostrzegają. Gdy dochodzi do zakłócenia, pierwszą porażką często nie jest reakcja, lecz rozpoznanie problemu. Ta linia podziału pokazuje, czy ryzyko zależności jest zamierzone i widoczne, czy odziedziczone i nieprzejrzyste.

Sygnały intencji: od analizy danych do prognozowania 4

Choć programy analizy wywiadowczej oparte na danych często sprawiają wrażenie kompleksowych, wnioski, które pojawiają się zbyt późno, nie wpływają już na decyzje. Ta linia podziału oddziela organizacje, które wykorzystują wczesne sygnały do ciągłego doskonalenia decyzji, wzmacniania zdolności przewidywania i stopniowego usprawniania reakcji, od tych, które uczą się dopiero wtedy, gdy szkody zostały już wyrządzone.

Pułapka długu technicznego: starsza architektura jako ryzyko strategiczne 5

Starsze architektury mogą wydawać się stabilne w codziennej działalności operacyjnej. W warunkach współczesnego tempa ataków i presji regulacyjnej stają się kruche, pochłaniając czas, talenty i odporność szybciej, niż organizacje są w stanie się adaptować. Ta linia podziału pokazuje, czy architektura umożliwia ewolucję, czy po cichu ją ogranicza.

Miraż chmury: oddzielenie narastającego ryzyka 6

Strategie chmurowe obiecują skalowalność i wydajność, ale współdzielone płaszczyzny zarządzania oraz ścisłe zależności koncentrują ryzyko awarii. Gdy pojawia się presja, systemy zawodzą jednocześnie. Pozwala to sprawdzić, czy odporność została zaprojektowana z myślą o ograniczaniu skutków, czy jedynie założona na podstawie planów odzyskiwania sprawności. Dojrzałe organizacje ograniczają skalę skutków i z każdym zakłóceniem zwiększają swoją odporność na awarie.

Spis treści

1

Okiełznanie algorytmu: zarządzanie SI na dużą skalę

Okiełznanie algorytmu: zarządzanie SI na dużą skalę

Wdrażanie SI przyspiesza szybciej, niż modele nadzoru w przedsiębiorstwach są w stanie się dostosować. To, co zaczęło się jako odizolowane eksperymenty, stało się elementem codziennego funkcjonowania, obecnym w przepływach pracy, narzędziach dla programistów, interakcjach z klientami oraz oprogramowaniu firm zewnętrznych, z którego organizacje korzystają, ale nad którym nie sprawują bezpośredniej kontroli. Zanim jednak SI zacznie działać samodzielnie, widoczność, odpowiedzialność i ograniczenia muszą być już wdrożone. Gdy decyzje zaczynają zapadać z szybkością maszyn, na dyskusję nad tymi kwestiami jest już za późno.

Choć większość zespołów kierowniczych uznaje sztuczną inteligencję za kwestię rozpatrywaną na poziomie zarządu, niewiele osób jest w stanie jasno określić, gdzie SI jest wykorzystywana, jakich danych dotyka ani w jaki sposób ryzyko jest zarządzane w całej organizacji. Ta luka między świadomością znaczenia SI a realną nad nią kontrolą jest dziś jednym z najbardziej brzemiennych w skutki martwych punktów współczesnego przywództwa.

Pytanie nie brzmi już, czy sztuczna inteligencja zapewnia wartość. Chodzi raczej o to, czy kierownictwo ma wystarczającą widoczność, by na dużą skalę zarządzać wpływem SI na odporność, zaufanie, koszty i odpowiedzialność.

SI nie jest już na etapie eksperymentów. Działa dziś w samym centrum przedsiębiorstwa i musi być zarządzana z taką samą dyscypliną, jak finanse, ryzyko i regulacje. W takim otoczeniu to pewność działania staje się rzeczywistym wyróżnikiem.

Szybkość wygrywa. Zgoda przegrywa.

Dostępność SI zasadniczo zmieniła sposób, w jaki technologia trafia do organizacji. Pracownicy i zespoły nie czekają już na scentralizowaną zgodę. Narzędzia SI są wdrażane po cichu, za pośrednictwem rozszerzeń przeglądarki, osadzonych funkcji SaaS, interfejsów API i platform programistycznych, często w dobrej wierze i z natychmiastowymi korzyściami dla produktywności.

Konsekwencje są przewidywalne: sztuczna inteligencja rozprzestrzenia się szybciej niż mechanizmy nadzoru. W praktyce 98% pracowników korzysta z niezatwierdzonych aplikacji w ramach zastosowań związanych z szarą strefą SI i szarą strefą IT[1].

Niezatwierdzone narzędzia wprowadzają niespójne środki kontroli bezpieczeństwa i niejasne praktyki przetwarzania danych, a także rozmywają odpowiedzialność. Dla zarządów tworzy to niewygodną rzeczywistość. Ryzyko związane ze sztuczną inteligencją jest istotne, ale często słabo kwantyfikowane i słabo zarządzane.

Nie świadczy to o braku dyscypliny. To strukturalne niedopasowanie między tradycyjnymi modelami zatwierdzania a bezbarierową krzywą wdrażania SI.

Nadzór nie może już być etapem zatwierdzania. Musi stać się stale działającym systemem opartym na mechanizmach zabezpieczających, ciągłej widoczności i standardach, które skalują się równie szybko jak wdrażanie SI.

Dane są zarówno zasobem o najwyższej wartości, jak i źródłem odpowiedzialności.

Systemy SI czerpią wartość z dostępu: do danych, do modeli i do dalszych decyzji. Pod presją szybkiego dostarczania rozwiązań organizacje często rozszerzają dostęp szybciej, niż wzmacniają kontrole. Granice uprawnień zacierają się. Przepływy danych stają się nieprzejrzyste. Usługi o niższym poziomie zaufania zyskują bliskość do informacji wrażliwych. Dziewięćdziesiąt siedem procent organizacji, które zgłosiły incydent bezpieczeństwa związany z SI w 2025 roku, nie miało odpowiednich mechanizmów kontroli dostępu do SI[2].

Tradycyjne ramy bezpieczeństwa nie zostały zaprojektowane pod kątem wychwytywania zagrożeń natywnych dla sztucznej inteligencji, takich jak manipulacja promptami, niezamierzone przechowywanie danych czy niewłaściwe wykorzystanie modeli. W rezultacie wiele organizacji może poświadczać zgodność, nie rozumiejąc w pełni narażenia na zagrożenia z powodu sztucznej inteligencji.

Takie ramy jak NIST AI RMF i ISO/IEC 42001 dostarczają wytycznych, ale rzeczywista pewność wynika z tego, w jaki sposób są wdrażane i egzekwowane. Każdy system SI jest najpierw systemem danych, a dopiero potem systemem inteligentnym. Jeśli liderzy nie potrafią odwzorować jego przepływów danych, ścieżek nadużyć i trybów awarii, nie jest on gotowy do skalowania.

> Za każdym razem, gdy proces decyzyjny zostaje zautomatyzowany, powtarza się ten sam schemat: skutki pojawiają się szybciej niż odpowiedzialność. Sztuczna inteligencja nie tworzy tej luki, ale ją ujawnia. Gdy odpowiedzialność jest niejasna, **nadzór staje się fasadowy**, niezależnie od tego, jak dopracowana wydaje się polityka".
>
> Joe Sullivan, były dyrektor ds. bezpieczeństwa, Uber

Szara strefa SI to szara strefa IT działająca z szybkością maszyn.

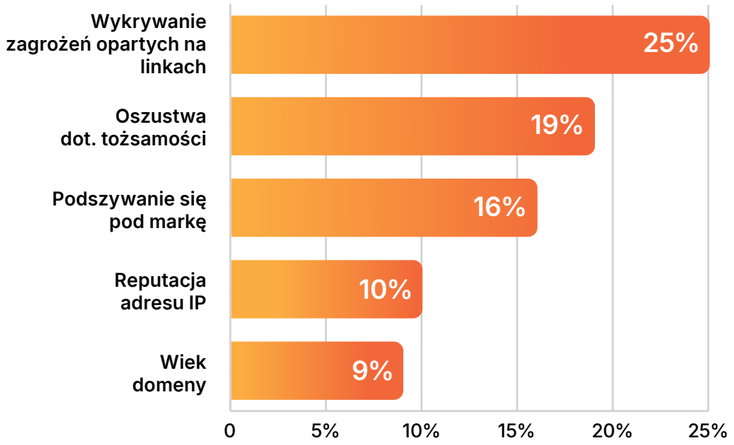
Sztuczna inteligencja może rozprzestrzeniać się niewidocznie wśród pracowników, podwykonawców, zespołów ds. produktu oraz dostawców zewnętrznych bez wyzwalania formalnego procesu weryfikacji. Powoduje to lukę w zakresie możliwości audytu dokładnie w momencie, gdy regulatorzy domagają się większej przejrzystości.

Rządy i organy regulacyjne coraz częściej wymagają udokumentowanych rejestrów systemów SI, możliwego do prześledzenia pochodzenia danych oraz możliwości wyjaśniania zautomatyzowanych decyzji. Niezdolność do wykazania kontroli szybko staje się naruszeniem zgodności, a nie jedynie oznaką niedojrzałości.

Wiodące organizacje uzupełniające tę lukę odchodzą od sporadycznych audytów na rzecz ciągłego zapewniania zgodności, łącząc kompleksowe rejestrowanie zdarzeń, zautomatyzowane gromadzenie dowodów oraz mechanizmy kontroli wykrywające w czasie rzeczywistym niezatwierdzone użycie SI.

Jeśli działań SI nie da się rejestrować, wyjaśnić i udokumentować, nie da się ich obronić przed organami regulacyjnymi, klientami czy zarządem.

Najczęściej wykrywane kategorie zagrożeń w poczcie e-mail



Wartości procentowe nie sumują się do 100%, ponieważ wiadomości e-mail mogą należeć do kilku kategorii zagrożeń jednocześnie.

Źródło: Cloudflare Radar

Ataki oparte na linkach i oszustwa związane z tożsamością dominują we współczesnych zagrożeniach związanych z pocztą e-mail. Kampanie te wykorzystują sygnały zaufania, a nie luki techniczne. W miarę jak SI obniża koszt tworzenia przekonujących, spersonalizowanych oszustw, mechanizmy zarządzania muszą wykraczać poza nadzór nad modelami i obejmować również uwierzytelnianie, integralność tożsamości oraz możliwość prześledzenia procesu decyzyjnego.

> Mechanizmy zarządzania zwykle wydają się wystarczające **aż do momentu, gdy wydarzy się coś nieoczekiwanego**. W przypadku SI taki moment nadchodzi wcześniej i ma szersze konsekwencje. Organizacje, które dobrze sobie z tym radzą, traktują sztuczną inteligencję mniej jak narzędzie, a bardziej jak łańcuch dostaw, śledząc pochodzenie, odpowiedzialność i wpływ, nawet gdy znajduje się ona poza ich strukturami".
>
> Kate Kuehn, globalna dyrektorka ds. strategii cyberbezpieczeństwa, World Wide Technology.

Regulacje są zapisane w kodzie, a nie tylko w zasadach.

Jurysdykcje na całym świecie zdecydowanie zwróciły się ku egzekwowalnym systemom nadzoru nad SI, które równoważą innowacyjność z odpowiedzialnością. W samych Stanach Zjednoczonych ustawodawcy stanowi przedstawili 1208 projektów ustaw dotyczących SI, co przełożyło się na uchwalenie 145 nowych ustaw w ciągu jednego roku[3]. Konsekwencje coraz częściej wykraczają poza same kary finansowe i obejmują również odpowiedzialność osobistą oraz powierniczą.

To sygnalizuje szerszą zmianę: nadzór nad SI jest ujmowany na nowo jako ryzyko na poziomie całego przedsiębiorstwa oraz odpowiedzialność kierownictwa, a nie jako uznaniowa polityka techniczna. Organizacje, które traktują mechanizmy zarządzania SI jak element infrastruktury, przekształcają zaufanie w czynnik wspierający wzrost, a nie w ograniczenie.

> Obserwujemy największe w historii rozprzestrzenianie się szarej strefy IT, ponieważ pracownicy korzystają z nienadzorowanych usług i agentów SI. W przeciwieństwie do szarej strefy IT w tradycyjnych rozwiązaniach SaaS, te funkcje SI są trudne do wykrycia lub zablokowania; mogą przyjmować rzeczywiste tożsamości użytkowników, wtapiać się w standardowe działania i działać z szybkością maszyn. Zadaniem dyrektora ds. bezpieczeństwa informacji nie jest blokowanie tego wdrożenia, lecz projektowanie bezpiecznych rozwiązań SI, które eliminują potrzebę korzystania z narzędzi nieobjętych nadzorem".
>
> Michael Goodman, wiceprezes oraz dyrektor ds. cyfryzacji i bezpieczeństwa (CD i SO), Hitachi

PYTANIA DLA WYŻSZEJ KADRY ZARZĄDZAJĄCEJ

Ujawnianie martwych punktów w zakresie nadzoru nad SI

Przy szybkości maszyn niejasno przypisana odpowiedzialność, ograniczona widoczność i słabe mechanizmy zabezpieczające stają się obciążeniem biznesowym, dlatego pytania te stają się imperatywem dla kierownictwa.

Pyt. 1

Kto na poziomie wykonawczym jest formalnie odpowiedzialny za nadzór nad SI?

A gdzie ta odpowiedzialność się zaczyna, a gdzie kończy? Czy została ona przełożona na konkretne działania operacyjne, czy jest jedynie zakładana, dopóki coś nie pójdzie nie tak?

Pyt. 2

Jakie ograniczenia określają dziś akceptowalne zachowanie SI w naszej organizacji?

Czy te ograniczenia są jasno sformułowane, jednoznaczne, możliwe do wyegzekwowania i spójne we wszystkich zespołach, czy w dużej mierze opierają się na zaufaniu, że nasi pracownicy będą przestrzegać zasad?

Pyt. 3

W jaki sposób oceniamy, czy wykorzystanie SI jest właściwe, a nie tylko zgodne z wymogami?

Czy zastosowania SI są zgodne z wymogami, ale jednocześnie nie są zgodne z intencjami biznesowymi, zasadami etycznymi lub poziomem akceptowalnego ryzyka? Czy zarządzamy rezultatami, czy jedynie dostępem i narzędziami? Jak odróżnić zgodność od niezgodności?

Pyt. 4

Gdyby jutro przeprowadzono audyt, czy potrafilibyśmy wykazać pełny, wspólny rejestr zastosowań SI w całym przedsiębiorstwie?

A może definicje, wykorzystanie w szarej strefie oraz ekspozycja na podmioty zewnętrzne ujawniłyby luki w naszym rozumieniu?

Pyt. 5

Czy w miarę przyspieszania wdrażania sztucznej inteligencji nasz model zarządzania pozostaje spójny?

Czy też ulega on rozproszeniu między funkcjami, dostawcami i regionami? Czy zarządzanie jest traktowane jak statyczne ramy, czy jak żywy system operacyjny?

2

Zaufanie w erze szybkości maszyn: projektowanie autonomii

Zaufanie w erze szybkości maszyn: projektowanie autonomii

Przedsiębiorstwa wchodzą w najbardziej doniosłą transformację od czasu komercjalizacji Internetu. Wyszliśmy poza etap narzędzi wspomaganych przez SI i wkroczyliśmy w erę „autonomicznego przedsiębiorstwa", w której agenty SI oraz agentowe przepływy pracy realizują kompleksowe procesy biznesowe przy minimalnej lub zerowej ingerencji człowieka. Ta linia podziału zakłada, że systemy SI są już wdrożone i działają autonomicznie. W odróżnieniu od wyzwania związanego z zarządzaniem SI, które koncentruje się na widoczności, nadzorze i odpowiedzialności, ta linia podziału dotyczy tego, co dzieje się po przekazaniu uprawnień maszynom. Pytanie nie dotyczy już tego, gdzie wykorzystywana jest sztuczna inteligencja ani kto za nią odpowiada; chodzi o to, czy zaufanie utrzyma się wtedy, gdy decyzje będą podejmowane bez udziału człowieka.

Gartner przewiduje, że do 2026 roku niemal połowa aplikacji korporacyjnych będzie zawierać wyspecjalizowane agenty SI przeznaczone do konkretnych zadań, podczas gdy jeszcze rok wcześniej poziom wdrożenia pozostawał jednocyfrowy[4]. Ta zmiana przynosi bezprecedensową szybkość i efektywność, ale jednocześnie wprowadza ryzyko o charakterze strukturalnym: decyzje biznesowe zaczynają wyprzedzać ludzki nadzór.

Zaufanie nie może mieć już charakteru okresowego, ręcznego ani retrospektywnego. W środowisku autonomicznym zaufanie musi być ciągłe, możliwe do zweryfikowania i egzekwowane z szybkością maszyn. Zabezpieczenie tej przyszłości wymaga fundamentalnej zmiany, od podejścia „ufaj, ale weryfikuj" do „zaufania wpisanego w projekt", a ostatecznie do systemów, które stają się coraz bardziej godne zaufania w miarę, jak są testowane.

Paradoks prędkości — gdy biznes rozwija się szybciej niż mechanizmy nadzoru

Tradycyjne podejście do bezpieczeństwa zakłada upływ czasu. Pojawia się alert. Człowiek przeprowadza analizę. Zapada decyzja. Systemy autonomiczne eliminują to okno czasowe. Agenty SI mogą wykonywać tysiące działań, takich jak rekonfiguracja infrastruktury, równoważenie portfeli i dostosowywanie łańcuchów dostaw, w ciągu milisekund. Jeśli agent SI zostanie przejęty, okaże się niewłaściwie ukierunkowany lub po prostu będzie działał błędnie, skutki pojawią się, zanim człowiek zdąży zareagować.

To jest paradoks prędkości: ta sama autonomia, która tworzy wartość, jednocześnie gwałtownie zmniejsza margines błędu. Atakujący to rozumieją. Phishing, podszywanie się i manipulacja oparte na SI są coraz częściej wymierzone w zautomatyzowane przepływy pracy, a nie w ludzi.

Wniosek jest jasny: bezpieczeństwo nie może funkcjonować poza systemem. Musi być osadzone bezpośrednio w samej warstwie decyzyjnej i regulować intencję, a nie tylko dostęp. Ta linia podziału nie dotyczy przewidywania ataków. Chodzi o zapewnienie, że gdy własne systemy podejmują działania, robią to w granicach świadomie wyznaczonych przez kierownictwo.

Nowa płaszczyzna zarządzania autonomiczną SI

1. Tożsamość musi obejmować nie tylko ludzi

Tożsamości inne niż ludzkie — agenty SI, konta usług, boty — przewyższają dziś liczbę użytkowników będących ludźmi o rzędy wielkości. Boty odpowiadają za około 30% ruchu HTTP obsługiwanego przez Cloudflare[5], a zdumiewające 92% wszystkich prób logowania obserwowanych przez Cloudflare pochodzi od botów — często są to ataki typu „credential stuffing"[6]. A jednak większość przedsiębiorstw nadal zarządza tożsamością, tak jakby to ludzie byli głównymi aktorami.

Ryzyko jest poważne. Systemy SI są często wdrażane bez silnego uwierzytelniania, odpowiednio ograniczonej autoryzacji oraz mechanizmów kontroli cyklu życia. W przypadku naruszenia bezpieczeństwa działają ze skalą rażenia właściwą dla maszyn.

Każdy agent SI musi mieć możliwą do zweryfikowania tożsamość kryptograficzną, nadzorowaną w ramach systemu zarządzania tożsamością maszyn. Dane uwierzytelniające muszą być krótkotrwałe, kontekstowe i możliwe do unieważnienia w czasie rzeczywistym. Autonomia bez tożsamości oznacza rezygnację z odpowiedzialności.

Rozkład żądań HTTP od botów (automatycznych) i od ludzi

Źródło: Cloudflare Radar

Nie działamy już w Internecie zorientowanym przede wszystkim na człowieka. Algorytmy coraz częściej wchodzą w interakcje z innymi algorytmami, często bez bezpośredniego nadzoru człowieka. Modele zarządzania oparte na uwierzytelnianiu użytkowników i mechanizmach kontroli dostępu pracowników są niedopasowane do tej rzeczywistości.

2. Systemy probabilistyczne wymagają deterministycznych mechanizmów zabezpieczających

Systemy SI rozumują probabilistycznie. Bezpieczeństwo nie może. Choć agenty mogą optymalizować, negocjować lub rekomendować, zasady określające, co wolno im robić, muszą być bezwzględne. Zasad nie można domniemywać, muszą być egzekwowane.

Wiąże się to z następującymi wymaganiami:

- Zasada jako kod, która definiuje nienegocjowalne ograniczenia
- Warstwy egzekwowania w czasie rzeczywistym, które przechwytują zamiar przed wykonaniem
- Rozdzielenie podejmowania decyzji od autoryzacji

Prawdziwa autonomia istnieje tylko tam, gdzie granice są jasno określone, egzekwowane i zaprojektowane z wyprzedzeniem.

> Ludzki osąd pozostaje niezbędny, ale nie działa już z szybkością, jakiej wymagają systemy. W środowiskach, w których maszyny pozostają w ciągłej interakcji, **zaufanie musi być z założenia wpisane w projekt, egzekwowane i weryfikowane** — podobnie jak systemy bezpieczeństwa, na których polegamy, nie zwracając na nie uwagi, aż do chwili, gdy zawiodą".
>
> Oliver Newbury, starszy doradca, TPG

3. Zaufanie wymaga obserwowalności, a nie założeń

W miarę jak systemy SI adaptują się, dryfują i uczą, wczorajsza pewność szybko przestaje mieć znaczenie. Bez głębokiej obserwowalności liderzy nie są w stanie odróżnić uzasadnionego autonomicznego działania od manipulacji.

Nieautoryzowane, często niewidoczne wykorzystanie SI dodatkowo zwiększa ryzyko, wprowadzając do kluczowych operacji modele, przepływy danych i logikę decyzyjną pozostające poza nadzorem.

Uzasadnienie ekonomiczne

Wbudowanie sztucznej inteligencji i automatyzacji w operacje dotyczące bezpieczeństwa przynosi wymierne korzyści finansowe. Organizacje, które szeroko wykorzystują te możliwości, usuwają skutki naruszeń o 80 dni szybciej i obniżają średni koszt naruszenia o 1,9 mln USD w porównaniu z tymi, które z nich nie korzystają[7].

Korzyści wykraczają poza samo obniżenie kosztów. Przy wdrożonych silnych mechanizmach zabezpieczających liderzy zyskują pewność potrzebną do głębszego wdrażania automatyzacji w przepływach pracy o kluczowym znaczeniu dla przychodów, poprawiając szybkość reakcji, tempo obrotu kapitału i przewagę konkurencyjną. Autonomia oparta na skutecznym zarządzaniu staje się czynnikiem wspierającym wzrost, a nie jedynie mechanizmem kontroli ryzyka. Bezpieczeństwo z szybkością maszyn nie jest narzutem. To cena skalowania autonomii bez wprowadzania kruchości.

System przywództwa dla autonomii

Wzrost znaczenia systemów autonomicznych na nowo definiuje rolę dyrektora ds. bezpieczeństwa informacji, a w konsekwencji także zakres odpowiedzialności całej kadry kierowniczej najwyższego szczebla. Przywództwo w obszarze bezpieczeństwa nie polega już na ochronie systemów po podjęciu decyzji; chodzi o kształtowanie zaufania w środowiskach, w których maszyny działają samodzielnie.

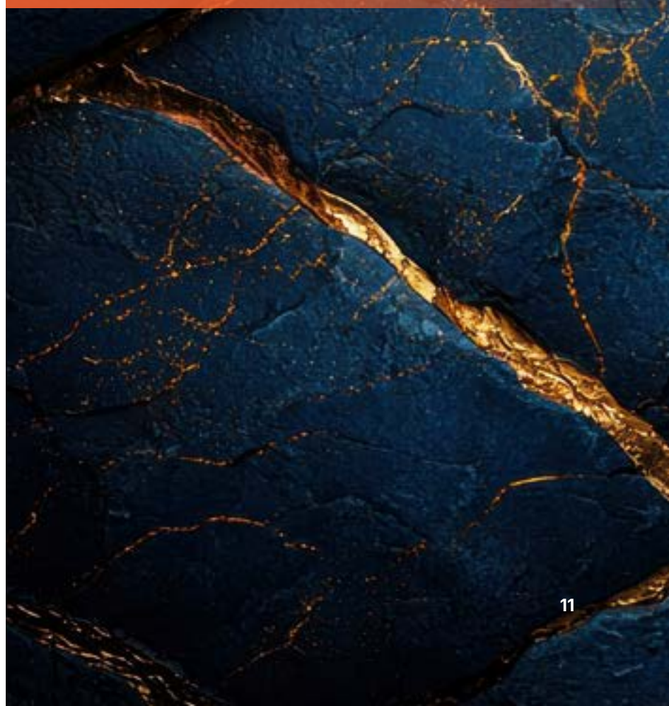
Pewien dyrektor ds. bezpieczeństwa informacji wspominał moment, gdy system SI po raz pierwszy samodzielnie wstrzymał transakcję wartą wiele milionów dolarów. Decyzja była właściwa, ale wywołała w sali posiedzeń rady nadzorczej głębsze pytanie: kto właściwie upoważnił maszynę do podjęcia takiej decyzji? Technologia wyprzedziła mechanizmy zarządzania.

Ta zmiana wymaga jasnych decyzji na poziomie kierownictwa: gdzie autonomia jest dopuszczalna, w jakim miejscu procesu decyzyjnego musi pozostać człowiek, jaki poziom przejrzystości jest wymagany w odniesieniu do modeli i danych oraz w jaki sposób mierzyć ryzyko, gdy decyzje podejmują maszyny.

Miary oparte na czasie reakcji człowieka już nie wystarczają. Liderzy muszą monitorować autonomiczne ryzyko, integralność decyzji oraz dryf systemowy. A jednak tylko około 15% zarządów przedsiębiorstw otrzymuje regularne wskaźniki dotyczące ryzyka i efektywności związane z SI[8].

W miarę jak autonomia się upowszechnia, obszary bezpieczeństwa, zgodności i technologii nie mogą już funkcjonować w izolacji. Bezpieczeństwo wpływa na dynamikę przychodów. Zgodność z przepisami warunkuje dostęp do rynku. Technologia definiuje odpowiedzialność. Zaufanie w erze szybkości maszyn nie jest programem bezpieczeństwa — to system przywództwa, który łączy odporność, zarządzanie, innowacyjność i reputację w ramach jednego mandatu zarządczego.

> Automatyzacja zmienia szybkość podejmowania decyzji, ale zmienia również skalę skutków błędów. Pytanie, przed którym stoją liderzy, brzmi: „Jak wbudować odpowiedzialność i zaufanie w systemy, które działają samodzielnie?"
>
> Kevin Jones, globalny dyrektor ds. bezpieczeństwa informacji, Bayer



PYTANIA DLA WYŻSZEJ KADRY ZARZĄDZAJĄCEJ

Przejście od automatyzacji do autonomii

Te pytania ujawniają, czy kierownictwo świadomie wyznaczyło granice wokół sposobu podejmowania decyzji z szybkością maszyn oraz to, jak odpowiedzialność za ryzyko jest przypisywana w czasie rzeczywistym.

Pyt. 1

Jakie decyzje korporacyjne są już podejmowane przez systemy autonomiczne?

Jakie decyzje świadomie pozostawiamy ludziom? Czy ta granica została świadomie zaprojektowana, udokumentowana i jest poddawana regularnemu przeglądowi, czy może jest jedynie domyślna i stopniowo się przesuwa?

Pyt. 2

Gdy maszyny działają samodzielnie, kto ponosi odpowiedzialność w czasie rzeczywistym — właściciel systemu, właściciel firmy czy sponsor na poziomie kierownictwa?

Czy odpowiedzialność za autonomiczne ryzyko jest jasno określona w trakcie działania systemu, czy analizuje się ją dopiero wtedy, gdy coś pójdzie nie tak?

Pyt. 3

Gdzie decyzje są podejmowane przez oprogramowanie, a nie przez ludzi?

W jakich obszarach poluzowaliśmy mechanizmy kontroli nad oprogramowaniem? Czy wobec maszyn stosujemy wyższe standardy niż wobec ludzi, czy po cichu obdarzamy je większym zaufaniem?

Pyt. 4

Czy potrafimy wyjaśnić i uzasadnić autonomiczne działanie w chwili, gdy ono zachodzi?

Czy też zajmuje to kilka dni później, dopiero podczas przeglądu incydentu? Czy intencja jest obserwowalna z szybkością maszyn, czy odtwarzana dopiero pod presją?

Pyt. 5

Czy nasz model zaufania skaluje się z szybkością maszyn?

Gdyby stopień autonomii podwoił się w ciągu najbliższego roku, czy nasz model zaufania wchłonąłby to przyspieszenie, czy załamałby się pod jego presją? Czy zaufanie zostało zaprojektowane z myślą o skalowalności i szybkości, czy odziedziczone po modelach zarządzania z epoki zdominowanej przez człowieka?

3

Ukryte łańcuchy dostaw: ujawnianie niewidocznych zależności

Ukryte łańcuchy dostaw: ujawnianie niewidocznych zależności

Nasza hiperpołączona gospodarka nie jest już definiowana przez to, co się kontroluje, ale przez to, co może doprowadzić do upadku, a czego nawet nie widać. Wielu liderów wzmocniło swoje granice ochrony, zmodernizowało infrastrukturę i zaostrzyło nadzór, jednak najpoważniejsze ryzyka znajdują się dziś poza ich polem widzenia, są osadzone w ekosystemach podmiotów zewnętrznych trzeciego, czwartego i kolejnych poziomów, których ani nie posiadają, ani nie są w stanie w pełni kształtować. Niewygodna prawda jest taka, że można być operacyjnie dojrzałym, a jednocześnie systemowo kruchym.

Ukryte łańcuchy dostaw nie są przypadkami marginalnymi, lecz naturalnym skutkiem cyfrowego składania systemów na dużą skalę. Każda integracja SaaS, każde wywołanie interfejsu API, każda biblioteka open source i usługa SI dodają kolejną warstwę dziedziczonego ryzyka. Pytanie dla liderów nie brzmi już: „Czy mamy ryzyko łańcucha dostaw?”, lecz: „Czy rozumiemy, która zewnętrzna awaria może już jutro zatrzymać przychody, podważyć zaufanie lub uruchomić kontrolę regulacyjną?”

Skutki są już dziś wymierne. Naruszenia związane z łańcuchem dostaw kosztują średnio 4,91 mln USD, czyli więcej niż globalna średnia dla naruszeń, wynosząca 4,44 mln USD[9]. Strategiczny wybór stojący przed liderami sprowadza się do tego, czy traktować ryzyko łańcucha dostaw jako ćwiczenie zgodności i godzić się na okresowe zaskoczenia, czy też uznać je za bieżącą ekspozycję operacyjną, wymagającą ciągłej widoczności, zapewniania bezpieczeństwa w czasie działania oraz zabezpieczeń dotyczących architektury.

Zagrożenie, które nigdy nie zostało zatwierdzone

Nowoczesne łańcuchy dostaw nie ograniczają się już do bezpośrednich dostawców. Obejmują także platformy SaaS, natywne usługi chmurowe, dostawców modeli SI, komponenty open source oraz warstwy infrastruktury podwykonawców, które funkcjonują daleko poza zasięgiem działów zaopatrzenia. Awarie w dowolnym miejscu tej rozbudowanej sieci, niezależnie od tego, czy chodzi o naruszenie bezpieczeństwa, przestój czy niezgodność z wymogami, mogą szybko doprowadzić do szkód po stronie klientów, narażenia regulacyjnego i zakłóceń o charakterze systemowym.

Podstawowym wyzwaniem jest widoczność, a sztuczna inteligencja zwiększa zarówno ryzyko, jak i nieprzejrzystość. Większość organizacji nie jest w stanie dostrzec swoich rozszerzonych, cyfrowych łańcuchów dostaw, a tym bardziej zarządzać nimi w czasie rzeczywistym. Każdy model SI, interfejs API i zautomatyzowany przepływ pracy po cichu rozszerza zależności poza tradycyjny nadzór. Audyty mają charakter statyczny, podczas gdy ryzyko jest dynamiczne.

Gdy systemy są składane, a nie budowane

Współczesny samochód powstaje dzięki pracy setek dostawców, a części sprzętowe, układy scalone i oprogramowanie pochodzą od wielu producentów, z których każdy ma własny łańcuch dostaw. Mała ukryta wada może przy dużej prędkości stać się problemem bezpieczeństwa, dlatego producenci samochodów inwestują znaczne środki w identyfikowalność i ciągłe testowanie.

Środowisko IT w przedsiębiorstwach coraz bardziej odzwierciedla dziś ten model. Jedna aplikacja może zależeć od dziesiątek narzędzi SaaS, usług w chmurze, interfejsów API, bibliotek open source i modeli SI, z których dla każdego istnieją podrzędni podwykonawcy i dostawcy usług. Przedsiębiorstwo widzi interfejs, nie warstwy ukryte pod spodem. To właśnie jest ukryty łańcuch dostaw.

Różnica tkwi w dyscyplinie. W branży motoryzacyjnej części są śledzone, a akcje przywoławcze prowadzi się precyzyjnie. W branży IT, gdy biblioteka lub komponent SI zostaje naruszony, wiele organizacji najpierw gorączkowo próbuje ustalić, czy są narażone. Coroczne ankiety nie są w stanie dotrzymać kroku systemom, które zmieniają się co tydzień. Widoczność i ciągłe zapewnianie zgodności stają się dla systemów cyfrowych równie istotne, jak kontrola jakości w przypadku samochodów.

Trzy czynniki przyspieszają wzrost tego ryzyka:

- **Model oparty na zaufaniu pośrednim stał się domyślnym modelem operacyjnym.** Przedsiębiorstwa ufają swoim dostawcom. Dostawcy ufają swoim dostawcom. Niewiele podmiotów weryfikuje cały łańcuch. Względy konkurencyjne i ograniczona widoczność wewnętrzna sprawiają, że podłańcuchy dostaw rzadko są szczegółowo ujawniane.
- **SI wprowadziła nową, nieprzejrzystą warstwę zależności.** Pracownicy coraz częściej polegają na narzędziach generatywnej SI oraz usługach z wbudowaną SI, które narażają dane wrażliwe na kontakt z modelami dostawców czwartego poziomu. Zespoły odpowiedzialne za ryzyko związane z podmiotami zewnętrznymi często nie mają jasności co do tego, w jaki sposób te modele wykorzystują dane, jak długo przechowują informacje ani czy uczą się na danych wejściowych przedsiębiorstwa, co zwiększa ryzyko regulacyjne, ryzyko dotyczące własności intelektualnej oraz ryzyko związane z suwerennością danych.
- **Wymogi regulacyjne stają się coraz bardziej rygorystyczne.** Na całym świecie organy regulacyjne zdecydowanie przechodzą od wytycznych do egzekwowania przepisów. Coraz częściej oczekuje się od organizacji wykazania widoczności zależności od podmiotów zewnętrznych trzeciego i czwartego poziomu, szczególnie tam, gdzie w grę wchodzą dane osobowe, dane finansowe lub infrastruktura krytyczna. Wybiegając w przyszłość, od liderów będzie się oczekiwać nie tylko oceny ryzyka dostawców, lecz także ilościowego określania ryzyka operacyjnego wynikającego z rozszerzonych łańcuchów dostaw. Efekt? Rosnąca luka między tym, czego oczekują regulatorzy, a tym, co organizacje są obecnie w stanie wykazać.

10 marek, pod które najczęściej podszywają się cyberprzestępcy w kampaniach phishingowych

1	Windows	6	Amazon
2	SANS	7	Instagram
3	Microsoft	8	Costco
4	Stripe	9	YouTube
5	Facebook	10	iCloud

Źródło: próby podszywania się zaobserwowane przez Cloudflare Email Security

Marki, pod które najczęściej podszywają się cyberprzestępcy, nie są przypadkowymi celami. To podstawowe platformy osadzone w przepływach pracy przedsiębiorstw — dostawcy tożsamości, systemy płatności, platformy chmurowe i systemy operacyjne. Atakujący wykorzystują znajomość tych marek i zależność od nich, zamieniając zaufaną infrastrukturę cyfrową w wektor ataku. Ukryte łańcuchy dostaw to nie tylko ekspozycja operacyjna, lecz także ekspozycja związana z tożsamością i marką.

Od statycznego zapewniania zgodności do ciągłej przejrzystości

Rozwiązanie problemu ukrytego łańcucha dostaw nie wymaga dodatkowej papierkowej roboty. Wymaga innego modelu operacyjnego. Przyszłość zapewniania bezpieczeństwa łańcucha dostaw to ciągła przejrzystość, czyli widoczność w czasie rzeczywistym tego, co faktycznie działa, jest połączone i wymienia dane w całym ekosystemie.

Jeden z dyrektorów ds. bezpieczeństwa informacji opisał sytuację, w której istnienie kluczowego dostawcy odkryto dopiero po pojawieniu się nietypowego ruchu w logach sieciowych. Dostawca był legalny, ale nikt nie zdawał sobie sprawy, jak głęboko jest osadzony w środowisku. Wniosek był prosty: nie da się zarządzać tym, czego nie widać.

Ta zmiana już się dokonuje. Wykazy komponentów oprogramowania, Software Bill of Materials (SBOM) oraz standard Vulnerability Exploitability eXchange (VEX) przekształcają się z artefaktów zgodności w sygnały operacyjne Należy oczekiwać, że działy zakupów będą coraz częściej wymagać nie tylko umów, lecz także aktualnych, odczytywalnych maszynowo ujawnień mapujących komponenty, zależności i możliwość wykorzystania podatności wraz ze zmianami w czasie[10].

Jednocześnie egzekwowanie zabezpieczeń przesuwa się coraz bliżej miejsca, w którym ryzyko się materializuje. Środki kontroli na poziomie sieci i łączności pozwalają organizacjom obserwować zachowanie, wykrywać nieautoryzowane przepływy danych oraz identyfikować ukrytych dostawców w chwili, gdy taka aktywność występuje.

Zapewnianie bezpieczeństwa łańcucha dostaw staje się zdolnością operacyjną, a nie okresowym przeglądem. Zaufanie jest stale weryfikowane. Ryzyko zostaje ujawnione odpowiednio wcześnie. Nadzór działa w tym samym tempie co ekosystem, który ma chronić.

Ufaj, ale stale weryfikuj

30% naruszeń bezpieczeństwa w 2025 roku wiązało się z zaangażowaniem podmiotów zewnętrznych, czyli było ich dwa razy więcej niż rok wcześniej[11], co pokazuje, jak głęboko relacje w łańcuchu dostaw wpływają dziś na ekspozycję na ryzyko, wykraczającą poza tradycyjne granice wewnętrzne.

Jednak organizacje wiodące pod tym względem mają wspólną cechę: traktują ryzyko związane z łańcuchem dostaw jak system, a nie jak funkcję zgodności. Dążą do tego, by wiedzieć, jakie aplikacje istnieją i w jaki sposób są ze sobą połączone. Wymagają, aby przejrzystość przenikała w dół łańcucha dostaw, a nie kończyła się na pierwszej umowie. Wykorzystują sygnały na poziomie sieci do wykrywania ukrytej aktywności, zamiast polegać na samoocenie. Stosują zasady zero trust do dostępu między maszynami, a nie tylko wobec użytkowników. I nieustannie dokonują ponownej oceny ryzyka związanego z dostawcami na podstawie ich zachowania, a nie reputacji.

Korzyści są wymierne. 85% organizacji będących liderami w modernizacji aplikacji aktywnie ogranicza nadmiarowe narzędzia i szarą strefę IT, aby zmniejszyć powierzchnię narażenia na atak w łańcuchu dostaw i poprawić sprawność operacyjną[12]. Nie są to techniczne korekty, lecz decyzje przywódcze dotyczące tego, jak duży poziom niepewności organizacja jest gotowa tolerować w systemach, od których zależy każdego dnia.

> Ryzyko rzadko wynika z zależności, których wszyscy się spodziewają, **pojawia się raczej tam, gdzie nikt ich nie widzi**. Gdy widoczność jest niepełna, audyty dają poczucie bezpieczeństwa, ale zapewniają niewielką ochronę. Prawdziwa odporność wynika z architektury, która ujawnia swoje zależności w trakcie działania".
>
> Tim Brown, dyrektor ds. bezpieczeństwa informacji, SolarWinds

> **Wzajemnie połączone ekosystemy premiują szybkość i specjalizację, ale jednocześnie rozpraszają ryzyko w sposób, którego umowy nie są w stanie uchwycić. To wgląd operacyjny, a nie dokumentacja, ostatecznie pozwala ograniczać ekspozycję na ryzyko".**
>
> **Sandip Wadje, globalny dyrektor ds. ryzyka operacyjnego i analiz dotyczących wschodzących technologii, BNP Paribas**

PYTANIA DLA WYŻSZEJ KADRY ZARZĄDZAJĄCEJ

Zarządzanie ryzykiem, którego się nie kontroluje

Ryzykiem łańcucha dostaw nie da się już w pełni zarządzać. To ryzyko, z którym organizacje muszą funkcjonować. Trzeba zatem zdecydować, czy będzie ono widoczne i objęte nadzorem, czy nieprzejrzyste i po prostu przyjmowane jako założenie.

Pyt. 1

Które krytyczne procesy biznesowe musielibyśmy wstrzymać, gdyby zawiodła kluczowa zależność?

Czy wiedzielibyśmy, dlaczego się nie udało? Czy potrafimy w czasie rzeczywistym powiązać wpływ na przychody i klientów z konkretnymi zależnościami, czy też zorientowalibyśmy się co do skali ekspozycji dopiero wtedy, gdy szkody już by powstały?

Pyt. 2

Jak odpowiemy na pytania organów regulacyjnych lub zarządu dotyczące ryzyka związanego z ekosystemem?

Czy potrafimy odpowiedzieć na pytania o te ryzyka, nie odwołując się do umowy? Czy mamy techniczną widoczność operacyjnej ścieżki ryzyka związanego z dostawcą?

Pyt. 3

W których obszarach ograniczyliśmy widoczność łańcucha dostaw, aby zachować szybkość działania, wygodę lub relacje z dostawcami?

Czy są to świadome decyzje? Kto zdecydował o zaakceptowaniu tych kompromisów? Które zależności są w praktyce „wyłączone” spod kontroli?

Pyt. 4

Jak szybko jesteśmy w stanie ustalić, czy nowo ujawniona luka w zabezpieczeniach nas dotyczy?

Czy odpowiedzialność za reakcję jest wyraźnie przypisana? Czy wykrywanie ekspozycji mierzy się w minutach, dniach czy tygodniach?

Pyt. 5

Czy zarządzamy ryzykiem łańcucha dostaw jako ciągłym procesem, czy jako okresowym audytem?

Czy nasz model ewoluuje tak szybko jak nasz ekosystem, czy jedynie utwierdza nas w przekonaniu, że zeszłoroczne mechanizmy kontrolne zostały zweryfikowane?

4

Sygnały intencji: od analizy danych do prognozowania

Sygnały intencji: od analizy danych do prognozowania

Już pobieżny przegląd nagłówków pokazuje, że aktywność przeciwników stale rośnie, i to w coraz szybszym tempie oraz na coraz większą skalę. Dzięki rekonesansowi wspieranemu przez SI i gotowym zestawom narzędzi coraz więcej cyberprzestępców jest zdolnych do przeprowadzania ataków o większej skali i większym stopniu zaawansowania niż kiedykolwiek wcześniej. Dodatkowo okno czasowe między pojawieniem się zagrożenia a jego wpływem na biznes staje się coraz krótsze, ponieważ średni czas potrzebny przeciwnikowi na rozpoczęcie ruchu bocznego spadł do zaledwie 48 minut[13].

Analiza zagrożeń, niegdyś uznawana za zdolność o charakterze uznaniowym, stała się dziś elementem fundamentalnym. 52% organizacji utrzymuje obecnie wyspecjalizowane, wewnętrzne zespoły ds. analizy cyberzagrożeń (CTI)[14]. W szybko zmieniającym się krajobrazie zagrożeń ich analiza przestała być wyłącznie funkcją bezpieczeństwa, a stała się kompetencją przywódczą. O sukcesie decyduje zdolność analizowania danych CTI w kontekście biznesowym, odróżniania istotnych sygnałów od szumu oraz przekładania wiedzy na możliwe do wykorzystania przewidywania.

Analiza zagrożeń nie polega już na tym, by wiedzieć więcej. Chodzi o to, by wiedzieć, co ma znaczenie — *wystarczająco wcześnie, aby móc działać.*

Od sygnału taktycznego do sygnału strategicznego

Współczesne zagrożenia charakteryzują się dużą dynamiką, dużą skalą i są w coraz większym stopniu kształtowane przez geopolitykę, czynniki ekonomiczne oraz luki w zabezpieczeniach specyficzne dla branży. W tym środowisku analiza zagrożeń nie może być już traktowana jako opcjonalna funkcja bezpieczeństwa ani ograniczana do powierzchownych przeglądów ogólnych, zewnętrznych źródeł danych. Kontekst, na poziomie przedsiębiorstwa, branży i skali globalnej, ma znaczenie, a kadra kierownicza musi wymagać informacji, które bezpośrednio łączą aktywność zagrożeń z wpływem na działalność, narażeniem operacyjnym i ryzykiem strategicznym.

Mówiąc wprost, po stronie atakujących dzieje się zbyt wiele, by dało się na bieżąco śledzić wszystko. Skuteczna obrona wymaga szybkości i kompetencji, a często brakuje zarówno jednego, jak i drugiego. Choć strategia bezpieczeństwa powinna obejmować i uwzględniać pełny wykaz zasobów oraz zobowiązań pozostających pod Twoją ochroną, wykorzystanie analiz do zrozumienia nie tylko technicznych aspektów zagrożeń, ale także ich kontekstu, pozwala dostroić program bezpieczeństwa tak, aby w pierwszej kolejności ograniczać ryzyko w obszarach mających największe znaczenie dla Twojej organizacji.

Ustalenie, co jest istotne dla organizacji, zazwyczaj wymaga współpracy zarządu i kierownictwa co do sposobu integrowania podstawowych zasad biznesowych, sił rynkowych, przepisów oraz oczekiwań interesariuszy. Ten kontekst ma ogromną wartość przy ocenie analiz zagrożeń, ponieważ zapewnia perspektywę organizacyjną niezbędną do ustalenia, które dane CTI są najbardziej użyteczne.

To właśnie w ten sposób analizę zagrożeń można wykorzystać do „odfiltrowywania" zbędnych informacji, takich jak nieistotne podatności czy grupy atakujących, które celowo wymierzają działania w zupełnie inne branże. Dzięki temu można skoncentrować zasoby tam, gdzie mogą przynieść największy efekt, zgodnie z krajobrazem zagrożeń właściwym dla danej organizacji. Analiza zagrożeń, która nie wspiera decyzji kadry kierowniczej, jest po prostu szumem informacyjnym, który należy odfiltrować.

Branże będące celem największej liczby ataków DDoS w 2025 roku

Pozycja w rankingu	Branża
1	Hazard i gry
2	Telekomunikacja
3	Technologia i usługi
4	Bankowość i usługi finansowe
5	Handel detaliczny

Ten ranking przedstawia średnią dla obserwowanych globalnie ataków DDoS, zarówno na warstwie sieciowej, jak i na warstwie aplikacji. W przypadku warstwy sieciowej najwięcej ataków dotyczy sektora technologii i usług, w przypadku warstwy aplikacji — gry i hazard.

Źródło: Cloudflare Radar

Aktywność atakujących nie rozkłada się równomiernie. Przeciwnicy priorytetowo traktują sektory związane z wpływem ekonomicznym, stabilnością infrastruktury i znaczeniem geopolitycznym. Koncentracja na określonych branżach odzwierciedla strategiczną intencję, a nie przypadek. Skuteczna analiza zagrożeń pozwala przewidywać, gdzie presja będzie się nasilać, i odpowiednio dostosowywać mechanizmy obronne.

Analiza zagrożeń stała się koniecznością

W miarę dojrzewania analizy zagrożeń jej punkt ciężkości przesuwa się z wskaźników technicznych na znaczenie biznesowe. Kadra kierownicza oczekuje dziś, że analiza zagrożeń wyjaśni, które zagrożenia rzeczywiście mają znaczenie, w jaki sposób zmiany geopolityczne i branżowe wpływają na ekspozycję oraz gdzie występują obszary kruchości w operacjach, relacjach z partnerami i wśród pracowników. Pytanie nie brzmi już, czy inwestować w analizę zagrożeń, lecz jaki rodzaj analiz organizacja uznaje za priorytetowy i za co jest gotowa płacić.

Aby ująć rozmowy budżetowe we właściwe ramy, warto rozważyć, w których obszarach CTI przynosi Twojej organizacji największą wartość:

- **Potwierdzenie**, że inwestycje w bezpieczeństwo są dostosowane do profilu ryzyka organizacji
- **Ograniczenie** szumu operacyjnego poprzez skupienie obrony na najbardziej krytycznych zagrożeniach
- **Proaktywne** ograniczanie ryzyka zamiast reaktywnego reagowania na incydenty po ich wystąpieniu

Z punktu widzenia dyrektora finansowego analiza zagrożeń znajduje uzasadnienie nie w liczbie alertów, lecz w swojej zdolności do ograniczania prawdopodobieństwa i skutków istotnych zakłóceń biznesowych, takich jak przestoje, oszustwa, interwencje regulacyjne czy szkody reputacyjne. Na poziomie organizacyjnym wymaga to jasności. Doraźne rozwiązania i niedofinansowane funkcje analizy zagrożeń nie są w stanie dostarczać informacji na poziomie oczekiwanym przez kadrę kierowniczą ani rezultatów, które dzięki nim można osiągnąć.

Niezależnie od tego, czy jest dostarczana przez zespół wewnętrzny, zaufanych partnerów czy w modelu hybrydowym, zasada pozostaje taka sama: analiza zagrożeń musi być terminowa, osadzona w kontekście i przydatna decyzyjnie. Dane analityczne, które jedynie wyjaśniają, co wydarzyło się wczoraj, w niewielkim stopniu przyczyniają się do ochrony jutra. Dostawcy oferujący nową jakość widoczności, na przykład wczesny wgląd w infrastrukturę przeciwnika, jego intencje i przygotowania, zapewniają strukturalną przewagę.

> “Wskaźniki wyjaśniają to, co już się wydarzyło, natomiast intencja pokazuje, co nadejdzie później. Najbardziej wartościowa analiza zagrożeń łączy zachowanie, kontekst i motywację, **zamieniając odosobnione sygnały w przewidywanie**, na podstawie którego liderzy mogą działać, zanim dojdzie do szkód”.
>
> **Menny Barzilay, współzałożyciel i prezes (CEO), Percepto**

Poruszanie się po krajobrazie zagrożeń w 2026 roku

Kilka linii podziału omówionych w tym rozdziale znajduje odzwierciedlenie w publikacji ***2026 Cloudflare Threat Report***. Raport oparty na danych z globalnej sieci Cloudflare, która chroni 20% Internetu, pomaga liderom koncentrować się na ryzykach wymagających działania, a nie jedynie na świadomości ich istnienia.

Analiza opiera się na prostym założeniu: wysiłek atakującego w relacji do skutków. Najważniejsze zagrożenia to te, które przy minimalnym wysiłku powodują nieproporcjonalnie duży wpływ na działalność biznesową. W 2026 roku przejawia się to w trzech wzorcach:

- **Industrializacja ataków** — przejście od ręcznie prowadzonych włamań do zautomatyzowanego, niemal bezwysiłkowego skalowania ataków z wykorzystaniem własnej infrastruktury chmurowej organizacji
- **Włamania z wykorzystaniem tożsamości** — przekształcenie oprogramowania typu ransomware w zdarzenie logowania, a nie klasyczne włamanie
- **Łączność w łańcuchu dostaw** — wykorzystanie połączeń między środowiskami SaaS i API-first jako narzędzia ataku

Uzyskaj publikację ***2026 Cloudflare Threat Report***.

Uzyskaj raport

Brakujący składnik: modelowanie zagrożeń

Integracja analizy zagrożeń z działalnością w zakresie bezpieczeństwa umożliwia optymalizację we wszystkich aspektach działalności, a ścisła integracja z modelowaniem zagrożeń przenosi ją o krok dalej — do roli strategicznego czynnika napędzającego działania całego przedsiębiorstwa.

Choć coraz więcej organizacji uwzględnia ryzyko w procesie podejmowania decyzji i uwzględnia redukcję ryzyka w swoich długoterminowych celach strategicznych, tylko 37% z nich z powodzeniem sformalizowało i udokumentowało swoje procesy modelowania zagrożeń[15]. Modelowanie zagrożeń zapewnia wspólną taksonomię, która pozwala uzgodnić wspólne założenia dotyczące ryzyka między dyrektorem ds. bezpieczeństwa informacji (CISO), kadrą kierowniczą najwyższego szczebla i zarządem. Wymusza jasne określenie priorytetów dotyczących zasobów, prawdopodobieństwa naruszeń bezpieczeństwa oraz wpływu na firmę w przypadku nieskuteczności mechanizmów kontrolnych.

Perspektywa uzyskiwana w ramach ćwiczeń z modelowania zagrożeń jest celowo utrzymywana na wysokim poziomie ogólności, zarządy oczekują bowiem jasności co do ryzyka systemowego, pojawiających się trendów w obszarze zagrożeń oraz tego, czy organizacja znajduje się po właściwej stronie linii podziału zagrożeń. W ramach modelowania zagrożeń ryzyka nieodłączne są mierzone na podstawie prawdopodobieństwa i dotkliwości wpływu, w oparciu o priorytety organizacji. Czynniki, takie jak mechanizmy kontrolne bezpieczeństwa i wyniki audytów, w połączeniu z analizą zagrożeń stanowią podstawę do obliczania ryzyka rezydualnego.

Włączenie danych CTI do procesu modelowania zagrożeń pozwala na jego dalsze doprecyzowanie, zapewniając podstawę dla takich działań jak walidacja mechanizmów kontrolnych i threat hunting (polowanie na zagrożenia), które są istotnymi elementami proaktywnego podejścia do kwestii bezpieczeństwa. Ponadto dane analityczne dotyczące sektora mogą potwierdzić, czy mechanizmy obronne są odpowiednio wzmocnione wobec najbardziej prawdopodobnych przeciwników, a także dostarczyć decydentom mocnych przesłanek do planowania budżetu i strategii.

Bez modelowania zagrożeń analiza pozostaje na poziomie operacyjnym. Dzięki niemu zyskuje ona wymiar strategiczny.

> Dobra analiza ogranicza szum informacyjny. Doskonała analiza skutkuje zmianami decyzji. Różnica polega na tym, czy pomaga liderom przewidywać kolejne ruchy, a nie tylko je wyjaśniać”.
>
> Troy Wilkinson, Venture Advisor, YL Ventures

Zaledwie

37%

organizacji pomyślnie sformalizowało i udokumentowało swoje procesy modelowania zagrożeń[16].

PYTANIA DLA WYŻSZEJ KADRY ZARZĄDZAJĄCEJ

Analiza zagrożeń jako kompetencja przywódcza

Analiza zagrożeń, jeśli jest przeprowadzona właściwie, łączy bezpieczeństwo, ryzyko, operacje, finanse i strategię w spójny obraz ekspozycji oraz intencji, użyteczny z perspektywy kadry kierowniczej.

Pyt. 1

Czy chronimy to, co jest nam dobrze znane, czy to, co ma największe znaczenie?

Czy jednoznacznie dostosowaliśmy nasze mechanizmy obronne do zagrożeń, które w tym roku mogłyby zakłócić przychody, operacje lub zaufanie?

Pyt. 2

Jak wcześnie naprawdę dostrzegamy intencje przeciwnika?

W których obszarach wykrywamy ataki dopiero po wyrządzeniu szkód, zamiast dzięki analizie zagrożeń? Czy wyprzedzamy cykl zagrożeń, czy podążamy za nim?

Pyt. 3

Czy odprawy dotyczące zagrożeń wspierają podejmowanie decyzji, czy jedynie służą przekazywaniu informacji?

Czy te wnioski zmieniają priorytety, inwestycje lub apetyt na ryzyko w czasie rzeczywistym?

Pyt. 4

Które decyzje lub procesy biznesowe zakończyłyby się niepowodzeniem jako pierwsze, gdyby doszło do naruszenia bezpieczeństwa dotyczącego zaufanej osoby?

Czy projektowaliśmy przepływy pracy przy założeniu, że ludzki osąd może zostać zmanipulowany lub podszyty?

Pyt. 5

Jak szybko potrafimy skorygować nasze działania, gdy przeciwnicy zmieniają swoje schematy działania?

Jakie mechanizmy pozwalają nam przewidzieć nadchodzącą zmianę, zanim odczuje ją firma?

5

Pułapka długu technicznego: starsza architektura jako ryzyko strategiczne

Pułapka długu technicznego: starsza architektura jako ryzyko strategiczne

W 2026 roku dług techniczny stanowi istotne ryzyko biznesowe, które po cichu osłabia konkurencyjność. Już w 2025 roku organizacje działały na granicy wydolności, zarządzając ponad 130 nowymi lukami w zabezpieczeniach dziennie, z których niemal 40% otrzymało ocenę wysoką lub krytyczną[17]. W miarę jak SI jest coraz częściej wykorzystywana do celów ofensywnych, a starsze architektury stają się nie do obrony, organizacje korzystające z rozproszonych stosów technologicznych ryzykują utknięcie w cyklu reaktywnego bezpieczeństwa, ograniczonej innowacyjności i rosnącej ekspozycji na ryzyko.

Dług techniczny stał się ujawnioną powierzchnią narażenia na atak, która zwiększa ryzyko szybciej, niż zespoły ludzkie są w stanie reagować. Organizacje, które zdecydowanie postawią na modernizację, nie tylko ograniczą ryzyko, lecz także zyskają szybkość, pewność działania i zdolność adaptacji, niezbędne do konkurowania w gospodarce opartej na sztucznej inteligencji.

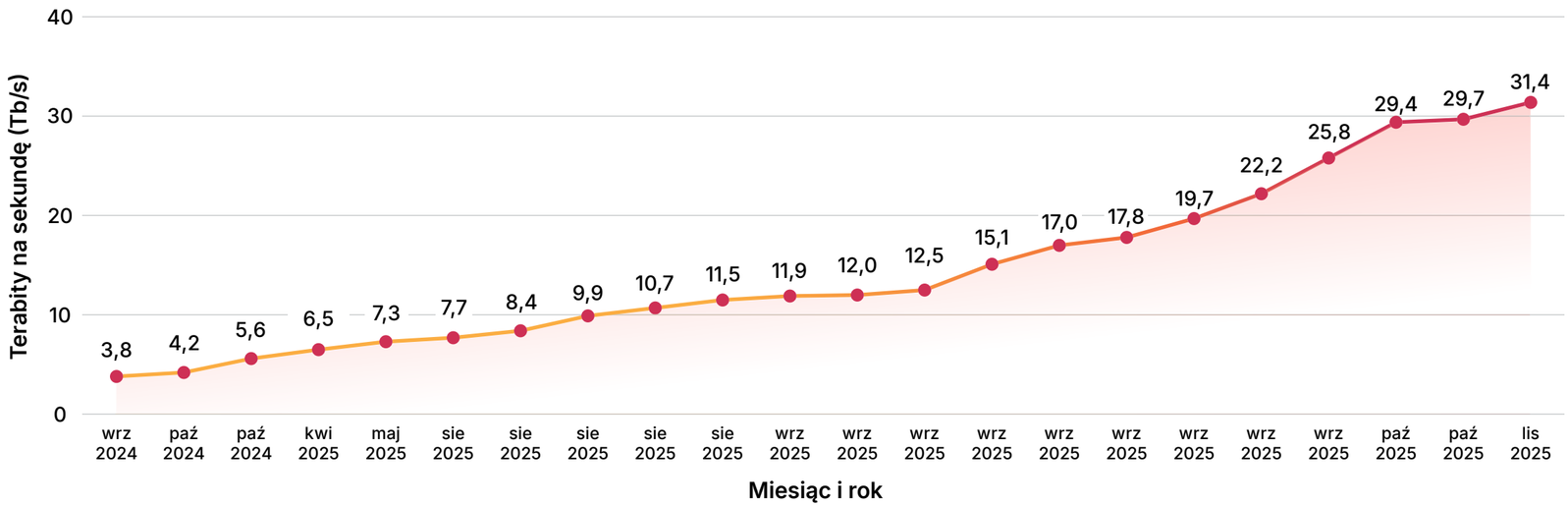
Gdy szybkość obnaża słabość strukturalną

Zmianą definiującą rok 2026 nie jest liczba luk w zabezpieczeniach, lecz tempo, w jakim są one wykorzystywane. Agentowa SI jeszcze bardziej skróciła czas między ujawnieniem podatności a jej wykorzystaniem, umożliwiając przeciwnikom identyfikowanie luk w zabezpieczeniach i ich operacyjne wykorzystanie w ciągu dni, a coraz częściej także w ciągu godzin.

Dane są jednoznaczne. W 2025 roku zaobserwowano aktywne wykorzystywanie 884 luk w zabezpieczeniach, a 29% z nich wykazywało oznaki wykorzystania już w dniu ich opublikowania[18]. Skala tego zjawiska jest równie bezprecedensowa. W przypadku React2Shell, jednej z najbardziej znanych luk w zabezpieczeniach w tym roku, odnotowano ponad miliard prób wykorzystania w ciągu zaledwie 11 dni[19].

Eskalacja bez gotowości dotyczącej architektury

Rekordowe ataki DDoS na świecie



Źródło: Cloudflare Radar

W ciągu nieco ponad roku liczba odnotowanych ataków DDoS wzrosła niemal dziesięciokrotnie. Scentralizowane, ściśle powiązane systemy nigdy nie były projektowane z myślą o takiej skali. Dług techniczny przekłada się dziś bezpośrednio na systemową kruchość w warunkach presji działającej z prędkością maszyn.

Starsze środowiska nie wytrzymują presji. Poważne awarie często występują wtedy, gdy współdzielone zależności zawodzą w tym samym czasie. Lata doraźnych poprawek doprowadziły do powstania ukrytego długu technicznego: niewidocznych integracji, kruchych interfejsów API i systemów, których aktualizowanie wiąże się ze zbyt dużym ryzykiem. Te środowiska nie zostały zaprojektowane z myślą o zagrożeniach działających z prędkością maszyn ani o ciągłej weryfikacji.

To ujawnia również ograniczenia 30-, 60- i 90-dniowych cykli poprawek. Zagrożenia są wykorzystywane w ciągu godzin, a nie kwartałów. Ochrona musi przesunąć się na brzeg sieci, aby ograniczać ekspozycję, zanim jeszcze dojdzie do kontaktu z podatnymi systemami.

> Atakujący nie rozróżniają starych i nowych systemów, lecz **szukają słabych ogniw.** Dług techniczny po cichu zwiększa liczbę tych ogniw, aż obrona staje się grą prawdopodobieństwa”.
>
> Jerry Perullo, założyciel, Adversarial Risk Management

Cykl niedoboru innowacji

Organizacje korzystające ze starzejących się stosów technologicznych są uwięzione w cyklu niedoboru innowacji. Wraz ze wzrostem kruchości infrastruktury rośnie liczba incydentów bezpieczeństwa. Wraz ze wzrostem liczby incydentów coraz większa część budżetu i zasobów kadrowych jest kierowana na konserwację. Skutkiem jest kurcząca się pula możliwości rozwoju.

Przeciętne przedsiębiorstwo globalne traci ponad 370 mln USD rocznie z powodu niezdolności do sprawnej modernizacji przestarzałych, nieefektywnych systemów i aplikacji[20]. Szacunki wskazują, że około 31% zasobów technologicznych jest przeznaczanych na obsługę długu technicznego[21]. Na prawdziwe innowacje, tj. nowe produkty, inicjatywy związane z SI i automatyzację, przypada zaledwie 7%. To nie stagnacja, lecz regres.

Podczas gdy liderzy wykorzystują SI do przyspieszania budowania przewagi konkurencyjnej, maruderzy płacą rosnącą „stopę procentową” od starego kodu, który ogranicza szybkość działania, odporność i elastyczność strategiczną.

Dlaczego starsze stosy zawodzą pod presją SI

Nowoczesne bezpieczeństwo zakłada automatyzację, integrację i kontrolę w czasie rzeczywistym. Starsze systemy opierają się na interwencji ręcznej, statycznych konfiguracjach i ochronie obwodowej. Ta rozbieżność staje się coraz bardziej niebezpieczna, ponieważ SI zmienia ekonomię zarówno ataku, jak i obrony.

Przestarzałe architektury borykają się z powolnym wdrażaniem poprawek, obciążonym długimi przestojami, ograniczoną widocznością interfejsów API i przepływów danych, rozproszonymi narzędziami, które nie potrafią koordynować reakcji, a także słabymi podstawami dla operacji opartych na SI. To często wymusza kompromis między ryzykiem cybernetycznym a ryzykiem operacyjnym, co odzwierciedla dobrze znane napięcie między dyrektorami ds. technicznych a dyrektorami ds. bezpieczeństwa informacji w sytuacji, gdy wdrażanie poprawek mogłoby zakłócić działanie firmy. Skutkiem jest opóźnienie, a właśnie opóźnienia są tym, co zagrożenia działające z prędkością maszyn potrafią wykorzystywać najlepiej.

Organizacje opóźniają wdrażanie SI nie dlatego, że brakuje im ambicji, lecz dlatego, że ich infrastruktura nie jest w stanie bezpiecznie jej obsłużyć. Tymczasem konkurenci dysponujący unowocześnioną architekturą pozwalają, by inicjatywy związane z SI popychały modernizację do przodu, wykorzystując rzeczywiste obciążenia robocze do uzasadniania i przyspieszania odnowy architektury. Na przykład 62% organizacji będących liderami innowacji aplikacyjnych uważa, że śledzenie bieżącego poziomu zgodności z wymogami bezpieczeństwa jest „bardzo łatwe”, w porównaniu z 35% organizacji pozostających w tyle względem harmonogramu[22].

370 mln USD

strat rocznie z powodu braku możliwości sprawnej modernizacji przestarzałych, nieefektywnych systemów i aplikacji[23]

Linia podziału w przywództwie

Różnica między liderami a maruderami sprowadza się do dyscypliny decyzyjnej. Organizacje, którym udaje się wyrwać z pułapki długu technicznego, wcześnie podejmują trudne decyzje. Centralizują odpowiedzialność za modernizację, łączą bezpieczeństwo z odpornością biznesową i traktują architekturę jako zasób strategiczny. 73% „liderów" modernizacji scentralizowało proces podejmowania decyzji, powierzając go zaledwie kilku osobom, w porównaniu z zaledwie 36% „maruderów"[24]. Ci, którym się to nie udaje, pozostają uwięzieni w paraliżu decyzyjnym zdominowanym przez komitety, gdzie podatności rozprzestrzeniają się szybciej niż zapadają decyzje, ryzyko narasta, a plany są dyskutowane bez końca.

Dług techniczny często odzwierciedla dług organizacyjny. Rozproszona odpowiedzialność właścicielska, niejasno przypisana odpowiedzialność i odkładane decyzje powodują tę samą kruchość w przywództwie i modelach operacyjnych, jaka występuje w starszej infrastrukturze. W 2026 roku taka kruchość nie daje już szans na przetrwanie.

Modernizacja jako ograniczanie ryzyka: odzyskiwanie czasu

Wyjście z pułapki długu technicznego wymaga spojrzenia na modernizację jak na imperatyw odporności, a nie jak na cykl modernizacji IT. Modernizacja ogranicza ryzyko, zmniejszając powierzchnię narażenia na atak dzięki konsolidacji, umożliwiając automatyczne wdrażanie poprawek i automatyczną reakcję oraz sprawiając, że obrona i operacje oparte na SI stają się wykonalne na dużą skalę. Co równie istotne, pozwala przesunąć ograniczone zasoby inżynieryjne do zadań o wysokiej wartości, zamiast angażować je w niekończące się prace konserwacyjne.

Organizacje, które odnoszą sukces, nie modernizują się przez przebudowę wszystkiego od podstaw, lecz tworzą stabilny, jednolity fundament, w którym bezpieczeństwo, wydajność i innowacyjność wzajemnie się wzmacniają. Gdy taki fundament jest już zbudowany, systemy można szybko udoskonalać, skalować i dostosowywać, nie dokładając nowych warstw wrażliwości.

Potrzebna zmiana nie ma charakteru stopniowego. Wymaga zgodności na poziomie kierownictwa i zdecydowanego działania. Starszą architekturę należy traktować jako mierzalne ryzyko biznesowe, a nie techniczną niedogodność. Uprawnienia decyzyjne dotyczące modernizacji muszą zostać scentralizowane. Inicjatywy związane z SI powinny umożliwiać odnowę architektury, zamiast czekać na idealne warunki. Platformy trzeba skonsolidować, aby ograniczyć złożoność i przywrócić widoczność.

Ostatecznie modernizacja polega na odzyskaniu czasu: na innowacje, na reakcję i na konkurowanie, zanim narastające ryzyko podważy przewagę.

73%

„liderów" modernizacji scentralizowało proces decyzyjny, powierzając go niewielkiej grupie osób, w porównaniu z zaledwie 36% „maruderów"[25].

PYTANIA DLA WYŻSZEJ KADRY ZARZĄDZAJĄCEJ

Narastający koszt starszych systemów

Dług techniczny osłabia szybkość działania i odporność. Wiele firm wydaje więcej na utrzymywanie przeszłości niż na budowanie przyszłości.

Pyt. 1

Jakie możliwości biznesowe są dziś ograniczone przez dług techniczny?

Kto odpowiada za ich usunięcie i jaki jest harmonogram ograniczania tego ryzyka?

Pyt. 2

Jaka część wydatków na bezpieczeństwo jest przeznaczana na utrzymanie starszych systemów, a jaka na budowanie odporności?

Jaka powinna być docelowa proporcja tych wydatków w ciągu najbliższych 12–24 miesięcy?

Pyt. 3

Które inicjatywy priorytetowe są opóźnione z powodu ograniczeń architektury?

Jakie korzyści w obszarze przychodów, efektywności lub ograniczania ryzyka odkładamy w rezultacie na później?

Pyt. 4

Jakie są trzy najważniejsze inicjatywy służące ograniczeniu długu technicznego w tym roku?

Jak będziemy mierzyć postępy i rozliczać kadrę kierowniczą z odpowiedzialności?

Pyt. 5

Jakie są największe przeszkody w ograniczaniu długu technicznego?

Czy są to ograniczenia budżetowe, luki kompetencyjne, konkurujące ze sobą priorytety, czy niejasny podział odpowiedzialności? Którą z nich usuniemy najpierw?

6

Miraż chmury: oddzielenie narastającego ryzyka

Miraż chmury: oddzielenie narastającego ryzyka

W miarę jak przedsiębiorstwa konsolidują swoje środowiska wokół mniejszej liczby platform chmurowych, aby działać szybciej, wiele z nich po cichu zwiększa ryzyko systemowe. Strategie oparte na jednej chmurze upraszczają operacje, ale koncentrują obszary awarii, podczas gdy środowisko wielochmurowe jest często traktowane jak pole wyboru do odhaczenia, a nie jak świadomie zaprojektowana strategia odporności.

Niedawne awarie sprawiły, że jednej prawdy nie da się już ignorować: o odporności nie decyduje liczba chmur wykorzystywanych przez organizację, lecz to, w jaki sposób zawodzi jej architektura. W 2026 roku liderzy muszą wyjść poza ideologię chmury i przyjąć podejście resilience-by-design — architektury zaprojektowane tak, aby ograniczać skutki awarii, zawężać promień rażenia i utrzymywać zaufanie w warunkach presji.

Gdy prędkość po cichu staje się kruchością

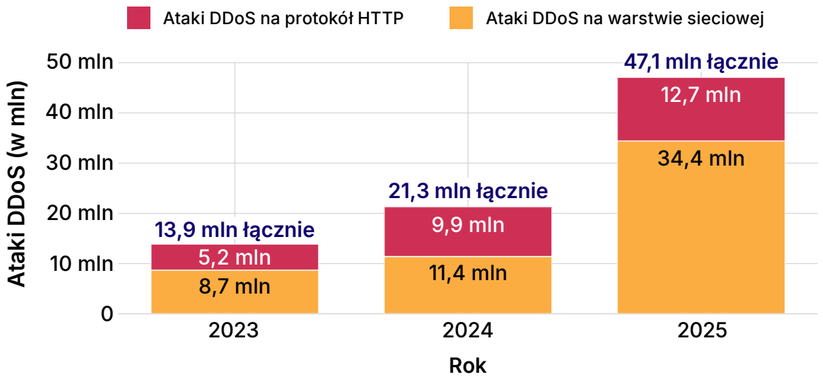
Celem nowoczesnego przedsiębiorstwa nie było tworzenie kruchych systemów. Wdrożenie chmury obiecywało szybkość, elastyczność i niezawodność, ale wprowadziło też mniej widoczne, bardziej systemowe ryzyko koncentracji, które trudniej ograniczyć pod presją.

Dzisiejsze awarie nie wynikają już wyłącznie z awarii po stronie jednego dostawcy. Incydent po stronie jednego dostawcy wciąż może być wyzwalaczem, ale najbardziej destrukcyjne zdarzenia występują wtedy, gdy współdzielone zależności zawodzą równocześnie — chodzi o systemy tożsamości, płaszczyzny zarządzania, potoki wdrożeniowe i usługi sieciowe stanowiące podstawę dla całej reszty. Wieloletnie dane Uptime Institute pokazują, że około dwie trzecie publicznie zgłaszanych awarii dotyczy zewnętrznych dostawców IT lub operatorów centrów danych, w tym gigantów chmurowych i internetowych, firm telekomunikacyjnych i dostawców usług kolokacyjnych[26].

Ciągłość działania zbyt często nadal koncentruje się na odtwarzaniu, skupiając się na przywracaniu usług, zamiast na ograniczaniu skutków awarii. Z czasem nakładające się warstwy zależności przekształcają środowiska w ściśle sprzężone systemy, w których drobne awarie mogą wywoływać efekt kaskadowy. Ta kruchość zwykle uwidacznia się dopiero w sytuacji kryzysowej.

Stała presja

Ataki DDoS według roku i typu



Źródło: Cloudflare Radar

Aktywność DDoS wzrosła ponad trzykrotnie w ciągu dwóch lat. Zakłócenia na dużą skalę nie mają już charakteru incydentalnego, lecz ciągły. W ściśle powiązanych środowiskach utrzymująca się presja zewnętrzna ujawnia ukryte zależności i wzmacnia drobne awarie, przekształcając je w zdarzenia systemowe. Odporność musi uwzględniać ciągły stres, a nie rzadkie awarie.

> Chmura zapewnia skalę, **ale nie daje automatycznie odporności.** Jeśli Twoje systemy zawodzą jednocześnie, nie została zaprojektowana żadna rzeczywista redundancja. Zaprojektowano korelację".
>
> **Mark Hughes, globalny partner zarządzający ds. usług cyberbezpieczeństwa, IBM**

Korzyści są oczywiste. Organizacje, które projektują i testują pod kątem awarii, osiągają znacznie lepsze wyniki. Jedna duża firma z sektora usług finansowych ograniczyła liczbę awarii o 40% i skróciła czas ich usuwania o niemal 60% po modernizacji architektury, poprawie obserwowalności i wdrożeniu podejścia zakładającego gotowość na awarie[27].

Dzisiejsze awarie wynikają nie tyle z problemów z chmurą, ile z erozji niezależności. Prawdziwym ryzykiem jest łączenie architektur. Odporność wymaga dziś celowej izolacji, ograniczania skali skutków awarii i traktowania ich powstrzymywania jako podstawowej zasady projektowej.

Iluzja jednej chmury: efektywność bez ograniczania skutków awarii

Dla wielu organizacji strategie oparte na jednej chmurze stały się domyślnym wyborem w dążeniu do efektywności. Standaryzacja narzędzi ogranicza złożoność, przyspiesza wdrożenia i obniża koszty operacyjne. Kompromisem jest ryzyko koncentracji. Ta sama konsolidacja, która zwiększa efektywność, może również centralizować awarię.

Główni dostawcy usług w chmurze są często bardzo odporni, ale dziś większe ryzyko ma charakter architektoniczny i operacyjny. Gdy tożsamość, egzekwowanie zasad, obserwowalność i potoki dostarczania opierają się na tej samej płaszczyźnie zarządzania lub tej samej granicy zaufania, odporność staje się założeniem, a nie wbudowaną właściwością systemu. Pojedynczy błąd, niezależnie od tego, czy leży po stronie dostawcy, czy klienta, może szeroko się rozprzestrzenić, jeśli architektura nie ogranicza jego skutków. Plany naprawcze mogą istnieć, ale rzeczywiste ograniczanie skutków awarii często już nie. Gdy coś się psuje, zbyt wiele elementów psuje się jednocześnie.

Dane branżowe potwierdzają tę rzeczywistość. Badania firmy Gartner pokazują, że większość awarii chmurowych wynika z błędnej konfiguracji i problemów operacyjnych, a nie z usterek samej infrastruktury. Analizy oparte na ankietach firmy Gartner wskazują, że około 80% incydentów bezpieczeństwa w chmurze wynika z błędnej konfiguracji, a prognozy sugerowały, że do ubiegłego roku nawet 99% awarii środowisk chmurowych będzie wiązać się z błędem ludzkim na którymś etapie tego łańcucha[28]. Wniosek nie jest taki, że ludzie popełniają błędy, bo to nieuniknione, lecz taki, że architektury muszą być projektowane tak, aby bezpiecznie absorbować skutki tych błędów.

Implikacje praktyczne są oczywiste. Odporność musi być projektowana, a nie zakładana z góry. Oznacza to projektowanie systemów tak, by w równym stopniu ograniczały skutki awarii, jak i umożliwiały odzyskiwanie sprawności, rozdzielanie krytycznych zależności, wdrażanie zabezpieczeń i zasad definiowanych w kodzie w celu ograniczenia skutków błędów oraz regularne testowanie scenariuszy awarii. Ryzyko koncentracji nie zniknęło w erze chmury. Przesunęło się na wyższe warstwy stosu technologicznego. Odporne pozostają te organizacje, które dopilnowują, by pojedyncza awaria nie przekształciła się w zdarzenie systemowe.

Mit środowisk wielochmurowych: redundancja bez niezależności

Środowiska wielochmurowe są często przedstawiane jako remedium na ryzyko koncentracji. W praktyce często odtwarzają tę samą kruchość, tyle że rozłożoną między różne logotypy. Większość środowisk wielochmurowych współdzieli dostawców tożsamości, potoki CI/CD, narzędzia do nadzoru oraz zależności SaaS. Gdy te wspólne warstwy zawodzą, obietnica niezależności natychmiast znika. Właśnie dlatego analizy po incydentach tak często pokazują, że „nadmiarowe” systemy nigdy nie były naprawdę niezależne.

Odporność nie zależy od tego, ile chmur widnieje na diagramie. Chodzi o to, które warstwy zawodzą niezależnie pod presją, a które nie.

Projektowanie pod kątem ograniczania skutków awarii, a nie doskonałości

Projektowanie autonomiczne zaczyna się od założenia, że systemy będą zawodzić, i koncentruje się na tym, by utrzymywać skutki awarii w wyznaczonych granicach oraz wyciągać z nich użyteczne wnioski. Celem jest nie tylko odporność na wstrząsy, lecz także rozwój dzięki nim.

Ograniczanie skutków awarii właśnie to umożliwia. Oznacza to, że awaria w jednym obszarze nie rozprzestrzenia się automatycznie na inne. Odizolowana awaria ma ograniczony zakres, jasną przyczynę i możliwe do opanowania skutki. Nie powoduje jednoczesnego unieruchomienia systemów tożsamości, zasad, danych i operacji.

Organizacje szeroko wykorzystujące SI i automatyzację znacznie skróciły cykle naruszeń o **80 dni** i obniżyły średni koszt naruszenia o

1,9 mln USD[29]

W architekturze przejawia się to poprzez niezależność między warstwami tożsamości, zasad i wykonania, rozdzielenie płaszczyzn zarządzania oraz bezpieczne domyślnie zachowanie w warunkach niepewności. Awarie są nieuniknione. Priorytetem jest utrzymywanie ich w ograniczonym zasięgu, zapewnienie, by były zrozumiałe i możliwe do przetrwania, jak również wykorzystywanie ich do wzmacniania systemu. Wiodące organizacje to nie te, które nie mają żadnych incydentów, lecz te, które skutecznie ograniczają promień rażenia każdego pojedynczego zdarzenia.

Ograniczanie skutków awarii jako przewaga rozwojowa

Choć często jest postrzegane jako forma zabezpieczenia, rozdzielenie warstw wspiera szybkość i wzrost. W publikacji IBM „Cost of a Data Breach Report 2025” wykazano, że organizacje szeroko wykorzystujące SI i automatyzację skróciły cykl naruszenia o 80 dni i obniżyły średni koszt naruszenia o 1,9 mln USD[30].

Ograniczając skalę skutków, liderzy zachowują zaufanie klientów, regulatorów i inwestorów oraz utrzymują elastyczność potrzebną do pewniejszego wdrażania SI, szybszego wejścia na rynek i ograniczenia liczby eskalacji na poziom kierowniczy. Gdy awaria pozostaje ograniczona, liderzy zachowują zdolność decyzyjną.

Ograniczanie skutków awarii nie ma charakteru wyłącznie defensywnego. Umożliwia szybsze działanie i bardziej świadome podejmowanie ryzyka w niestabilnym otoczeniu.

Projektowanie z myślą o awarii na najwyższym poziomie

W miarę jak systemy cyfrowe stają się fundamentem strategii biznesowej, decyzja o rozdzieleniu lub powiązaniu infrastruktury staje się decyzją biznesową o wysokiej stawce.

Kadra kierownicza musi zmienić perspektywę, odejść od pytania, jak szybko możemy odzyskać sprawność, na rzecz pytania, co nigdy nie może zawieść jednocześnie. Wymaga to jasności co do współdzielonych płaszczyzn zarządzania, zależności związanych z tożsamością i potokami, a także dowodów testowania trybów awarii, a nie jedynie danych o dostępności. Ograniczanie skutków awarii należy do poziomu zarządu, ponieważ awaria systemowa jest ryzykiem biznesowym, którego nie można delegować. Musi być świadomie projektowane od góry, tak aby żadna pojedyncza awaria nie przekształciła się w zdarzenie obejmujące całą firmę, a każdy incydent wzmacniał system.

> “Atakujący szukają jednej słabości, aby wywołać kaskadę zdarzeń. Jeśli pojedyncze naruszenie przekształca się w zdarzenie obejmujące całe przedsiębiorstwo, to nie jest pech. To efekt projektu architektury”.
>
> Dave Trader, dyrektor ds. bezpieczeństwa informacji, HALO Branded Solutions

PYTANIA DLA WYŻSZEJ KADRY ZARZĄDZAJĄCEJ

Gdy usługa współdzielona ulega awarii, czy architektura ogranicza jej skutki?

Rozpatrywane łącznie, te pytania pokazują, czy przedsiębiorstwo potrafi ograniczać zakłócenia w czasie rzeczywistym, czy też jego stabilność nadal zależy od nadziei, heroicznych działań i odtwarzania po incydencie.

Pyt. 1

Które systemy krytyczne mogą ulec awarii bez zatrzymania działalności?

Czy potwierdziliśmy to w testach, czy istnieje to tylko w teorii?

→

Pyt. 2

Gdyby system tożsamości lub kluczowa platforma uległy awarii, jakie przychody zostałyby zatrzymane?

Czy znamy skalę skutków z wyprzedzeniem, czy dopiero po wystąpieniu zakłócenia?

→

Pyt. 3

Czy środowisko wielochmurowe rzeczywiście ogranicza ryzyko, czy tylko zwiększa złożoność i koszty?

Gdzie ograniczyliśmy zależność, a gdzie ona pozostaje?

→

Pyt. 4

Czy mierzymy zdolność ograniczania skutków awarii, czy tylko czas odtworzenia?

Czy nasze kluczowe wskaźniki efektywności nagradzają zapobieganie, czy reaktywne sprzątanie?

→

Pyt. 5

Czy możemy wyjaśnić zarządowi lub organom regulacyjnym ostatnią awarię?

Czy wpływ był ograniczony celowo, czy też przez szczęśliwy zbieg okoliczności?

WNIOSKI

Zasady przywództwa budujące trwałą przewagę

W świecie kształtowanym przez decyzje wspierane przez SI, systemy autonomiczne i głęboko współzależne ekosystemy cyfrowe sama odporność już nie wystarcza. Przewaga będzie wynikać ze zdolności systemów do wykrywania przeciążeń, adaptacji w czasie rzeczywistym, ograniczania skutków awarii i dalszego działania bez oczekiwania na interwencję człowieka. To właśnie nazywamy odpornością autonomiczną.

Ten raport nie stanowi wykazu zagrożeń. Wyznacza mandat przywódczy: identyfikowanie i usuwanie linii podziału wpisanych we współczesne przedsiębiorstwa. Te strukturalne słabości mogą wydawać się możliwe do opanowania w warunkach stabilnego funkcjonowania, ale bez zdecydowanego działania nieuchronnie ujawnią się pod presją. Przebiegają one pod warstwą wdrażania SI, zależności od chmury, starszej architektury, analizy zagrożeń i modeli operacyjnych zbudowanych z myślą o bardziej przewidywalnej epoce.

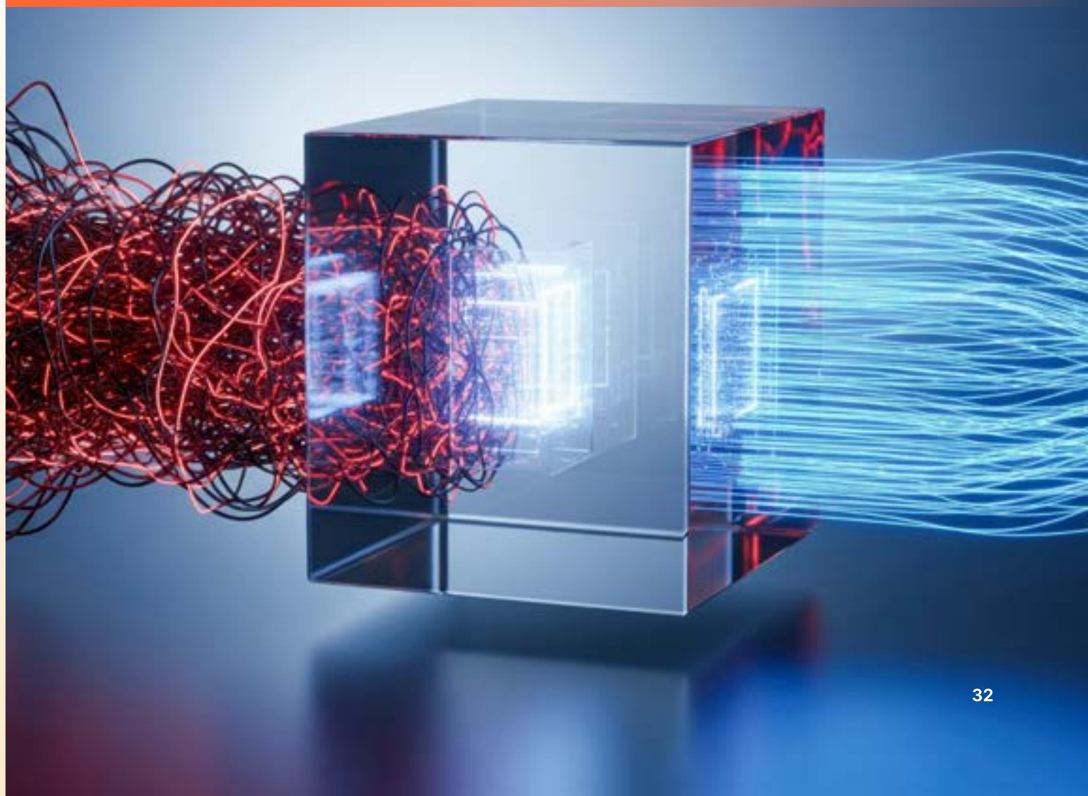
Konfrontowanie się z tymi liniami podziału nie jest wyłącznie zadaniem dyrektora ds. bezpieczeństwa informacji. Odporność autonomiczna jest obowiązkiem kadry zarządzającej wyższego szczebla, kształtowaną przez sposób, w jaki zespoły wykonawcze ustalają priorytety, przydzielają uprawnienia i projektują systemy, które same się regulują. Organizacje autonomiczne wyróżniają się zasadami, których konsekwentnie przestrzegają ich zespoły kierownicze:

- **Wspólna odpowiedzialność za ryzyko systemowe, zamiast delegowanej odpowiedzialności.** Za ryzyko systemowe odpowiada zespół kierowniczy, a nie osoby, którym delegowano je w dół struktury organizacyjnej. Zakres odpowiedzialności jest jasno określony, odpowiedzialność właścicielska jest współdzielona przez całą kadrę zarządzającą wyższego szczebla, a zarządy angażują się poprzez rzeczywiste scenariusze i kompromisy, a nie statyczne raportowanie.
- **Wykonanie osadzone w systemach, zamiast deklarowanych intencji.** Decyzje mają znaczenie tylko wtedy, gdy są realizowane z prędkością maszyn. Kontrola nad modelami, danymi, promptami i autonomicznymi działaniami musi być osadzona tam, gdzie odbywa się wykonanie. Wszystko, co opiera się na dokumentacji, uzgodnieniach lub procesach ręcznych, nie będzie skalowalne.
- **Niezależność strukturalna, zamiast krótkoterminowej wygody.** To, co wydaje się efektywne w spokojnych warunkach, pod presją często okazuje się źródłem kruchości. Zespoły o autonomicznej odporności nadają priorytet ograniczaniu skutków awarii, odwracalności i rozdzieleniu. Systemy są projektowane tak, aby awarie pozostawały lokalne, obserwowalne i możliwe do skorygowania. Zdolność do zapobiegania efektom kaskadowym staje się przewagą strategiczną.
- **Możliwe do udowodnienia zaufanie, zamiast zakładanej kontroli.** Zaufanie musi dać się stale potwierdzać, a nie być domyślnie zakładane. Liderzy wymagają wglądu w zachowanie systemów, egzekwowalnych mechanizmów kontroli obejmujących tożsamości ludzi i maszyn oraz dowodów integralności z szybkością maszyn. Domyślnie zakładane zaufanie zawodzi w warunkach autonomii.
- **Uczenie się na podstawie awarii, zamiast ich unikania.** Awaria jest oczekiwana i świadomie wykorzystywana jako źródło informacji. Wczesne wykrywanie, ograniczony promień rażenia, szybkie przywracanie sprawności i organizacyjne uczenie się wyznaczają skuteczność przywództwa. To szybkość przywracania sprawności, a nie zapobieganie, jest miarą, która ma znaczenie.

W roku 2026 przywództwo definiuje się już mniej przez planowanie stabilności, a bardziej przez projektowanie z myślą o zakłóceniach.

Liderami będą te organizacje, których kadra kierownicza osadza te zasady w codziennych decyzjach, przekształcając zmienność w uczenie się, presję w postęp, a niepewność w przewagę.

Liderami będą te organizacje, których kadra kierownicza osadza te zasady w codziennych decyzjach, **przekształcając zmienność w uczenie się, presję w postęp, a niepewność w przewagę.**



O firmie Cloudflare

O FIRMIE CLOUDFLARE

Jedna platforma. Jedna programowalna sieć.

Ponad 330 miast
w ponad 125 krajach, w tym w Chinach kontynentalnych

↳ **Ponad 210 miast**
z procesorami graficznymi do wnioskowania SI na całym świecie

~50 ms
od ok. 95% światowej populacji podłączonej do Internetu

Około 13 tys. sieci
łączy się bezpośrednio z rozwiązaniami Cloudflare, w tym z dostawcami usług internetowych, dostawcami usług w chmurze i dużymi przedsiębiorstwami

477 Tb/s
rosnącej przepustowości sieci

O FIRMIE CLOUDFLARE

Pakiet bezpieczeństwa Cloudflare

Odporność i obrona brzegowa

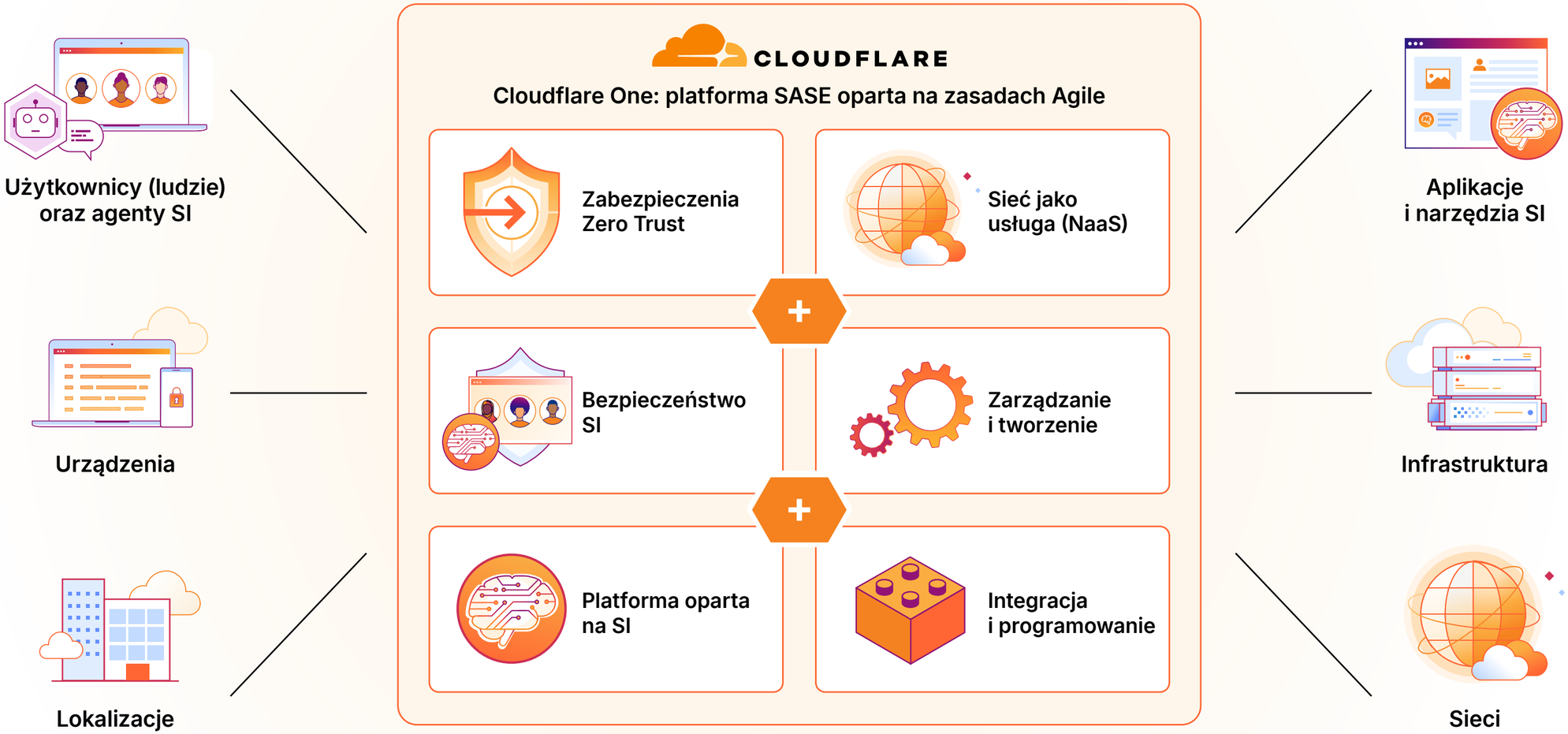
- Ochrona aplikacji internetowych i interfejsów API — blokowanie ataków, wychwytywanie luk w zabezpieczeniach i poprawianie dostępności
- Security Service edge (SSE) — egzekwowanie zabezpieczeń w modelu Zero Trust wśród pracowników hybrydowych
- Ochrona przed atakami DDoS — odpieranie największych, najbardziej zaawansowanych ataków dzięki przepustowości sieci na poziomie 477 Tb/s

Bezpieczna integracja chmury i sieci

- Secure Access Service Edge (SASE) — zapewnianie łączności i ochrony pracownikom, agentom SI oraz infrastrukturze
- Sieć jako usługa (NaaS) i środowisko wielochmurowe — łączenie, zabezpieczanie i przyspieszanie sieci korporacyjnych bez kosztów i złożoności związanych ze starszym sprzętem
- Połączenia międzysieciowe — bezpośrednie połączenie sieci lokalnej i sieci w chmurze z siecią Cloudflare

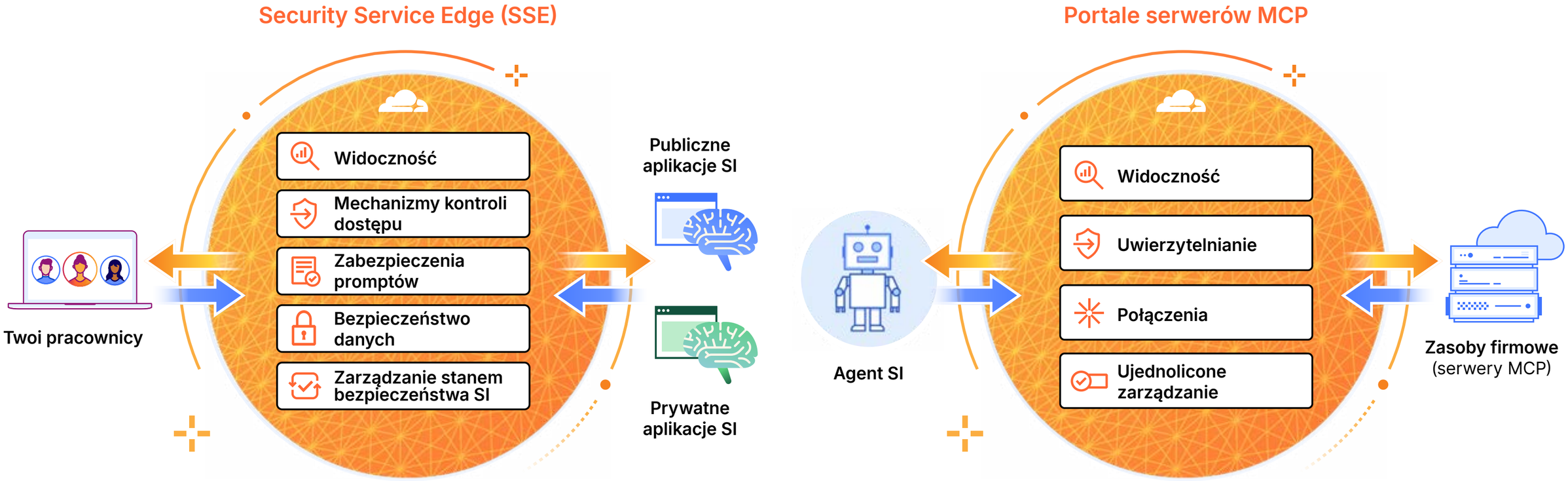
O FIRMIE CLOUDFLARE

Usługi Cloudflare One



O FIRMIE CLOUDFLARE

Ochrona korzystania z generatywnej SI oraz zarządzanie agentami SI



O FIRMIE CLOUDFLARE

Usługi Cloudflare AI w całym cyklu życia

Tworzenie SI
dzięki platformie programistycznej

Tworzenie SI w każdym regionie świata za pomocą jednego kliknięcia

Workers AI, Vectorize, AI Gateway

Tworzenie infrastruktury SI w trybie łatwym

Zdalny serwer MCP, pakiet Agents SDK, AI Search, AI Gateway

Ochrona wdrażania SI
za pomocą pakietu AI Security Suite

Zapewnianie bezpiecznego korzystania z generatywnej SI przez pracowników

Platforma SASE ***(Cloudflare One)***

Zarządzanie agentami SI

ZTNA firmy Cloudflare, w tym ***portale serwerów MCP***

Bezpieczne tworzenie SI

AI Gateway

Ochrona aplikacji opartych na SI

Zabezpieczenia aplikacji, w tym ***Firewall for AI***

Ochrona treści
za pomocą usług dotyczących aplikacji

Ochrona oryginalnych treści online przed robotami indeksującymi SI

Zarządzanie ruchem botów, w tym AI Crawl Control

Platforma oparta na SI w jednej sieci globalnej
Modele wykrywania zagrożeń · Agent SI (Cloudy) · Modele zapobiegania utracie danych

O FIRMIE CLOUDFLARE

Analizy dla nowoczesnego kierownictwa najwyższego szczebla

Poruszanie się w dzisiejszym krajobrazie zagrożeń i w warunkach szybkich zmian technologicznych wymaga czegoś więcej niż wiedzy operacyjnej — strategicznej dalekowzroczności. „The Executive Lens” to dedykowane centrum zasobów stworzone przez Cloudflare specjalnie dla liderów z kadry zarządzającej wyższego szczebla.

Poznaj opracowane przez ekspertów analizy, praktyczne ramy działania oraz unikalne badania na temat kluczowych zagadnień dotyczących przedsiębiorstw, takich jak cyberodporność, bezpieczny ład wokół SI oraz globalna transformacja cyfrowa.

Zapoznaj się z „The Executive Lens” już dziś.

Zobacz więcej informacji

Dodatkowe zasoby

Forrester Total Economic Impact

Wykrywaj zaawansowane zagrożenia i zapobiegaj nowym. Zobacz, jak Cloudflare pomaga przedsiębiorstwom wykorzystywać bezpieczeństwo jako przewagę konkurencyjną, działając w warunkach złożonego krajobrazu zagrożeń z większą wydajnością i przewidywalnością.

Zobacz więcej informacji

Security Signal

Oddziel to, co istotne, od informacyjnego szumu i skup się na najważniejszych dziś trendach w cyberbezpieczeństwie. Każdy odcinek „Security Signal” przekłada złożoność cyberbezpieczeństwa na praktyczne wnioski dla osób stojących na czele organizacji.

Obejrzyj teraz

2026 Cloudflare Threat Report

Poznaj krajobraz zagrożeń w 2026 r. określony przez nową miarę skuteczności (MOE). Raport opisuje nowe zagrożenia, w tym działania przygotowawcze sponsorowane przez państwa, kradzież tokenów, hiperwolumetryczne ataki DDoS i inne.

Zobacz więcej informacji

theNET

Analizy dotyczące innowacji w cyberbezpieczeństwie, krajobrazu zagrożeń i przyszłości Internetu, uzupełnione perspektywą kadry kierowniczej na temat rozwiązywania problemów organizacyjnych za pomocą technologii.

Zobacz więcej informacji

Kontakty

	Globalne	Ameryki	EMEA	Azja i Pacyfik	Japonia
Przywództwo rynkowe	 **Mark Anderson** Prezes ds. przychodów markanderson@cloudflare.com	 **Rick Congdon** Regionalny wiceprezes na obszar obu Ameryk congdon@cloudflare.com	 **Tony Van den Berge** Regionalny wiceprezes na obszar EMEA tonyberg@cloudflare.com	 **Goran Risticevic** Regionalny wiceprezes na obszar APAC goran@cloudflare.com	 **Sayoko Matsumoto** Regionalny wiceprezes w Japonii sayoko@cloudflare.com
Terenowy zespół CXO	 **Ramy Houssaini** Dyrektor ds. rozwiązań cybernetycznych ramy@cloudflare.com	 **Khalid Kark** Terenowy dyrektor ds. informatycznych, Ameryki khalid@cloudflare.com	 **Christian Reilly** Terenowy dyrektor ds. informatycznych, EMEA creilly@cloudflare.com	 **Volker Rath** Terenowy dyrektor ds. bezpieczeństwa informacji volker@cloudflare.com	 **Koichiro Otobe** Terenowy dyrektor ds. technicznych w Japonii koichiro@cloudflare.com

CLOUDFLARE

2026

Cloudflare Security Signals Report

Odporność autonomiczna

+44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/pl-pl/

REV:BDES-8897.2026MAR19

Przypisy końcowe

1. Jonathan Villa, „Hidden Risks of Shadow AI”, Varonis, www.varonis.com/blog/shadow-ai. Dostęp: 11 lutego 2026 r.
2. IBM, „Cost of a Data Breach Report 2025”, www.ibm.com/reports/data-breach. Dostęp: 11 lutego 2026 r.
3. MultiState, „Artificial Intelligence (AI) Legislation”, www.multistate.ai/artificial-intelligence-ai-legislation. Dostęp: 11 lutego 2026 r.
4. Gartner, „Gartner Predicts 40% of Enterprise Apps Will Feature Task-Specific AI Agents by 2026, Up From Less Than 5% in 2025”, 26 sierpnia 2025, www.gartner.com/en/newsroom/press-releases/2025-08-26-gartner-predicts-40-percent-of-enterprise-apps-will-feature-task-specific-ai-agents-by-2026-up-from-less-than-5-percent-in-2025. Dostęp: 11 lutego 2026 r.
5. Cloudflare Radar, „Bot Traffic”, radar.cloudflare.com/bots?dateRange=12w. Dostęp: 11 lutego 2026 r.
6. Cloudflare Radar, „Application Layer Security”, radar.cloudflare.com/security/application-layer?dateRange=12w. Dostęp: 11 lutego 2026 r.
7. IBM, „Cost of a Data Breach Report 2025”.
8. Lareina Yee, et al., „The AI Reckoning: How Boards Can Evolve”, McKinsey & Company, 24 października 2024, www.mckinsey.com/capabilities/mckinsey-technology/our-insights/the-ai-reckoning-how-boards-can-evolve. Dostęp: 11 lutego 2026 r.
9. IBM, „Cost of a Data Breach Report 2025”.
10. ENISA, „SBOM Analysis - Towards an Implementation Guide”, grudzień 2025, www.enisa.europa.eu/sites/default/files/2025-12/SBOM%20Analysis%20-%20Towards%20an%20Implementation%20Guide_v1.20-Published.pdf. Dostęp: 11 lutego 2026 r.
11. Verizon, „2025 Data Breach Investigations Report (DBIR)”, www.verizon.com/business/resources/reports/dbir. Dostęp: 11 lutego 2026 r.
12. Cloudflare, „2026 Cloudflare App Innovation Report”, 2026, www.cloudflare.com/resource/g/app-innovation-report/2026. Dostęp: 11 lutego 2026 r.
13. CrowdStrike, „2025 Global Threat Report”, www.securityweek.com/wp-content/uploads/2025/02/CrowdStrikeGlobalThreatReport2025.pdf. Dostęp: 18 marca 2026 r.
14. SANS Institute, „SANS 2025 CTI Survey: Cyber Threat Intelligence Survey”, SOCRadar, maj 2025, socradar.io/wp-content/uploads/2025/05/SANS-2025-CTI-Cyber_Threat_Intelligence_Survey-SOCRadar.pdf. Dostęp: 11 lutego 2026 r.
15. SANS Institute.
16. SANS Institute.
17. Mohammed Khalil, „Vulnerabilities Statistics 2025: Record CVEs, Zero-Days & Exploits”, DeepStrike, 8 października 2025, deepstrike.io/blog/vulnerability-statistics-2025. Dostęp: 25 lutego 2026 r.
18. VulnCheck, „VulnCheck State of Exploitation 2026”, 21 stycznia 2026, www.vulncheck.com/blog/state-of-exploitation-2026. Dostęp: 11 lutego 2026 r.
19. Dane dotyczące globalnej sieci Cloudflare.
20. Pegasystems, „Average Global Enterprise Wastes More Than $370 Million Every Year Through Technical Debt, Says Research”, 14 października 2025, www.pega.com/about/news/press-releases/average-global-enterprise-wastes-more-370-million-every-year-through. Dostęp: 11 lutego 2026 r.
21. Protiviti, „Global Technology Executive Survey: Tech Debt a Major Burden”, www.protiviti.com/us-en/global-technology-executive-survey-tech-debt-major-burden. Dostęp: 11 lutego 2026 r.
22. Cloudflare, „2026 Cloudflare App Innovation Report”.
23. Pegasystems, „Average Global Enterprise Wastes More Than $370 Million Every Year Through Technical Debt, Says Research.”
24. Cloudflare, „2026 Cloudflare App Innovation Report”.
25. Cloudflare, „2026 Cloudflare App Innovation Report”.
26. Uptime Institute, „Uptime Annual Outage Analysis Report 2025”, 6 maja 2025, uptimeinstitute.com/about-ui/press-releases/uptime-announces-annual-outage-analysis-report-2025. Dostęp: 11 lutego 2026 r.
27. Nuno De la Torre, et al., „IT Resilience for the Digital Age”, McKinsey & Company, 20 czerwca 2023, www.mckinsey.com/capabilities/tech-and-ai/our-insights/tech-forward/it-resilience-for-the-digital-age. Dostęp: 11 lutego 2026 r.
28. Ashwin Chaudhary, „Managing Cloud Misconfigurations Risks”, Cloud Security Alliance, 14 sierpnia 2023, cloudsecurityalliance.org/blog/2023/08/14/managing-cloud-misconfigurations-risks. Dostęp: 11 lutego 2026 r.
29. IBM, „Cost of a Data Breach Report 2025”.
30. IBM, „Cost of a Data Breach Report 2025”.