CLOUDFLARE

KRÓTKI OPIS ROZWIĄZANIA

Pakiet Cloudflare AI Security Suite

Zabezpiecz interakcje SI poprzez kontrolę danych oraz zarządzanie ryzykiem na wszystkich etapach cyklu życia SI.

Bezpiecznie skaluj SI

Ryzyka związane z SI wymagają nowoczesnych zabezpieczeń

Twoje zespoły wykorzystują sztuczną inteligencję, aby szybciej wprowadzać innowacje, jednak wiąże się to z poważnymi zagrożeniami dla bezpieczeństwa. Dotychczasowe podejście polegające na blokowaniu SI lub dodawaniu złożonych rozwiązań punktowych przestaje się sprawdzać, ponieważ hamuje innowacje i ignoruje rzeczywistość:

- **85% pracowników** korzysta z narzędzi SI, zanim dział IT zdąży je zweryfikować[1].
- **93% pracowników przyznaje,** że wprowadza dane firmowe do narzędzi SI bez uzyskania zgody[2].
- **63% organizacji, które doświadczyły naruszenia bezpieczeństwa,** nie posiada żadnych polityk zarządzania SI[1].

Dowiedz się, jak wspierać swoje zespoły i czerpać korzyści z produktywności oferowanej przez SI, jednocześnie zachowując poziom bezpieczeństwa i kontroli wymagany przez Twoją organizację.

Ujednolicona platforma do zabezpieczania agentowej i generatywnej SI

Cloudflare oferuje Twojej organizacji jedną platformę umożliwiającą bezpieczne i pewne wdrażanie SI. Umożliwiamy liderom ds. bezpieczeństwa skuteczne zarządzanie ryzykiem, zespołom technologicznym zwiększanie produktywności, a inżynierom platformowym bezpieczne tworzenie rozwiązań — tak, aby wszyscy mogli wspólnie wprowadzać innowacje w bezpiecznym środowisku.

Zacznij pracę z pakietem Cloudflare AI Security Suite

Pakiet Cloudflare AI Security Suite jest dostępny w ramach ujednoliconej platformy służącej do zabezpieczania wykorzystania narzędzi SI w środowisku pracy oraz aplikacji dostępnych publicznie. Wykrywaj szarą strefę SI, chroń modele przed nadużyciami, zabezpieczaj dostęp agentów oraz zapobiegaj ujawnianiu danych w promptach, aby Twoje przedsiębiorstwo mogło bezpiecznie i efektywnie wprowadzać innowacje, z lepszą widocznością procesów i większą kontrolą.

Rozszerz widoczność

w aplikacjach SI, punktach końcowych interfejsu API oraz połączeniach agentów SI.

Ograniczaj ryzyko

dzięki mechanizmom zabezpieczającym, kontroli stanu bezpieczeństwa i łagodzeniu zagrożeń w czasie rzeczywistym

Chroń dane

dzięki ochronie promptów oraz środkom kontroli dostępu dla pracowników i agentów SI.

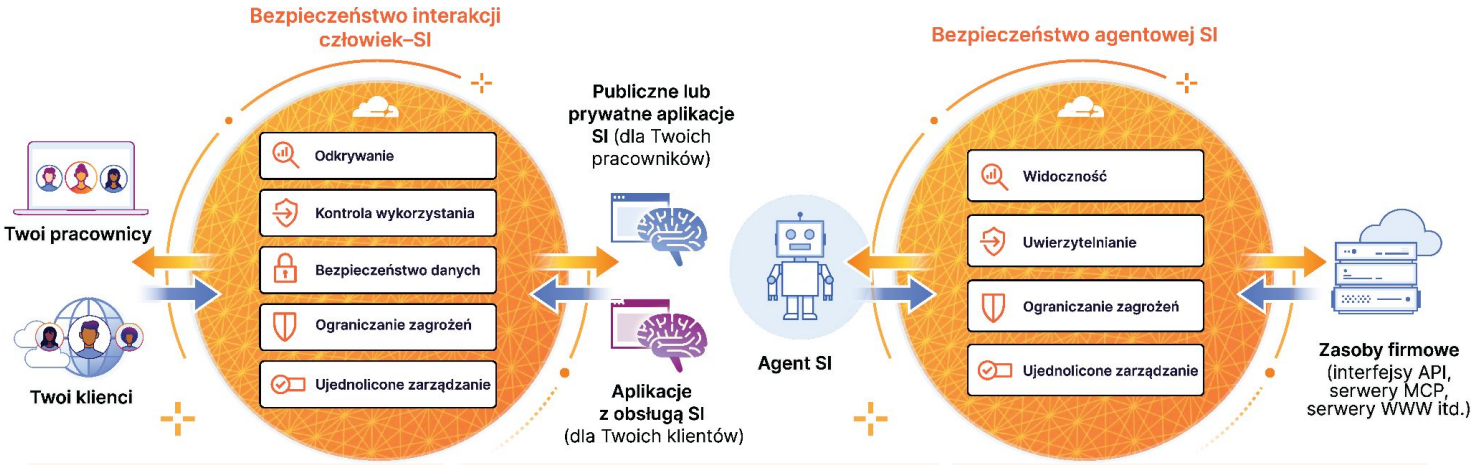
Bezpieczeństwo jest wbudowane
już na etapie tworzenia rozwiązań SI w środowisku Cloudflare.

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

REV:PMM-OCT2025

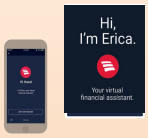
Zabezpiecz komunikację generatywnej i agentowej SI za pomocą pakietu Cloudflare AI Security Suite

Chroń całą komunikację związaną z SI poprzez kontrolę danych wykorzystywanych przez pracowników w generatywnej SI oraz zarządzanie zagrożeniami bezpieczeństwa wynikającym z działania autonomicznych agentów.



- **Twój personel:** pracownicy, podwykonawcy, programiści itd.
- **Twoi klienci:** odwiedzający Twoje witryny internetowe i aplikacje

- **Aplikacje generatywnej SI:** autonomiczne lub wbudowane Gemini, Claude, ChatGPT, Copilot
- **Aplikacje oparte na SI** Np. chatbot SI instytucji Bank of America o nazwie Erica



- **Interfejsy API** i **serwery MCP** dla dowolnej aplikacji Google Workspace
- **Serwery internetowe** na potrzeby wnioskowania i generowania rozszerzonego o wyszukiwanie (RAG)

Przyspiesz wdrażanie SI dzięki podejściu „security by design” w całym cyklu życia SI

Bezpieczne korzystanie z SI przez pracowników

Wdrażaj środki kontroli użycia SI oraz zarządzanie stanem bezpieczeństwa SI (AI-SPM), aby ograniczyć ryzyko i chronić dane.

Ochrona aplikacji opartych na SI

Chroń swoje aplikacje SI oraz interfejsy API przed atakami typu prompt injection i wyciekami danych w czasie rzeczywistym.

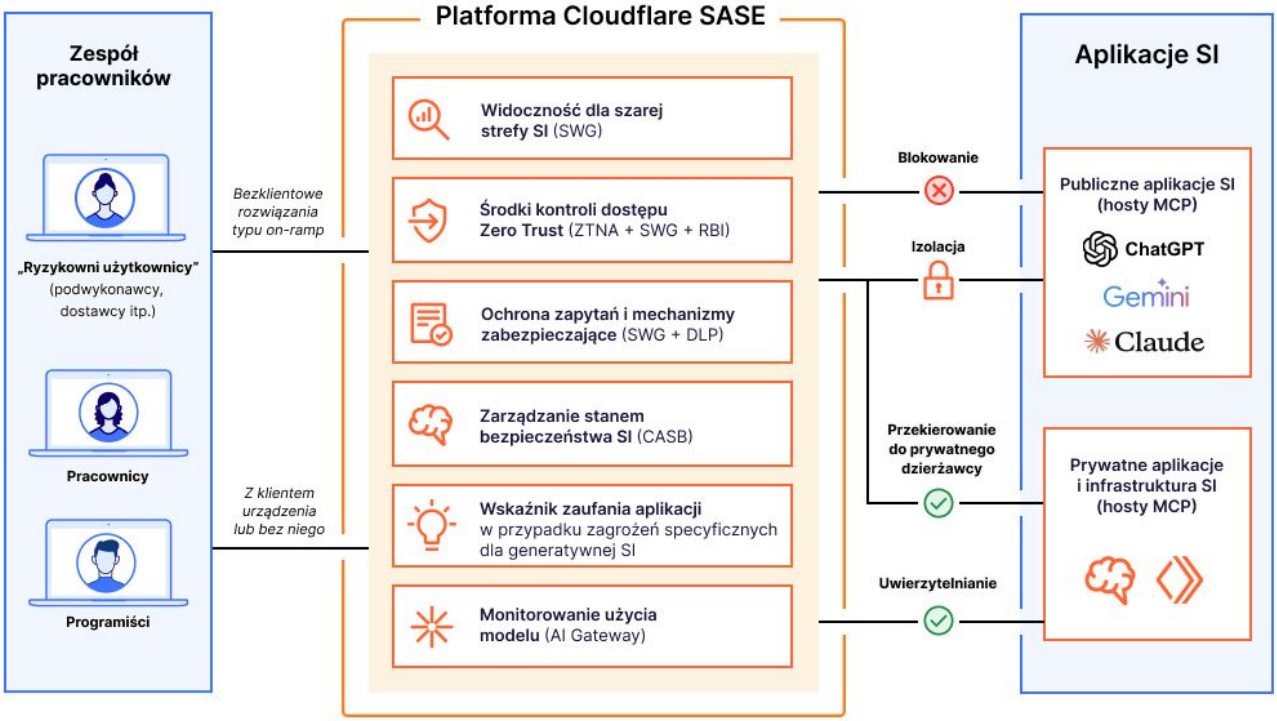
Bezpieczne tworzenie SI

Umożliwiaj programistom zabezpieczanie aplikacji SI dzięki zintegrowanym funkcjom obserwowalności, ograniczaniu częstotliwości żądań oraz wbudowanym zabezpieczeniom SI.

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

REV:PMM-OCT2025

Zabezpiecz pracowników korzystających z aplikacji i obciążeń obsługujących SI dzięki platformie SASE firmy Cloudflare



SSE chroni komunikację między człowiekiem a sztuczną inteligencją

- **Widoczność** — wykrywaj i analizuj wykorzystanie szarej strefy SI poprzez inspekcję ruchu in-line. Oceniaj ryzyko stwarzane przez te aplikacje SI, korzystając z transparentnej oceny.
- **Kontrola dostępu** — blokuj, izoluj, przekierowuj lub akceptuj połączenia użytkowników. Egzekwuj reguły modelu Zero Trust oparte na tożsamości dla każdej aplikacji.
- **Ochrona i zabezpieczenia promptów** — wykrywaj i blokuj prompty na podstawie intencji (np. próby złamania zabezpieczeń, nadużycia kodu, żądania danych umożliwiających identyfikację osoby).
- **Bezpieczeństwo danych** — powstrzymaj ujawnianie danych poufnych dzięki wspomaganej przez SI ochronie przed wyciekiem danych (DLP) obejmującej dane umożliwiające identyfikację osoby, kod źródłowy i inne.
- **Zarządzanie stanem bezpieczeństwa SI** — integracja z narzędziami generatywnej SI za pośrednictwem interfejsu API w celu skanowania pod kątem błędnych konfiguracji za pomocą naszego brokera zabezpieczeń dostępu do chmury (CASB). Dostępne teraz dla ChatGPT, Claude oraz Google Gemini.

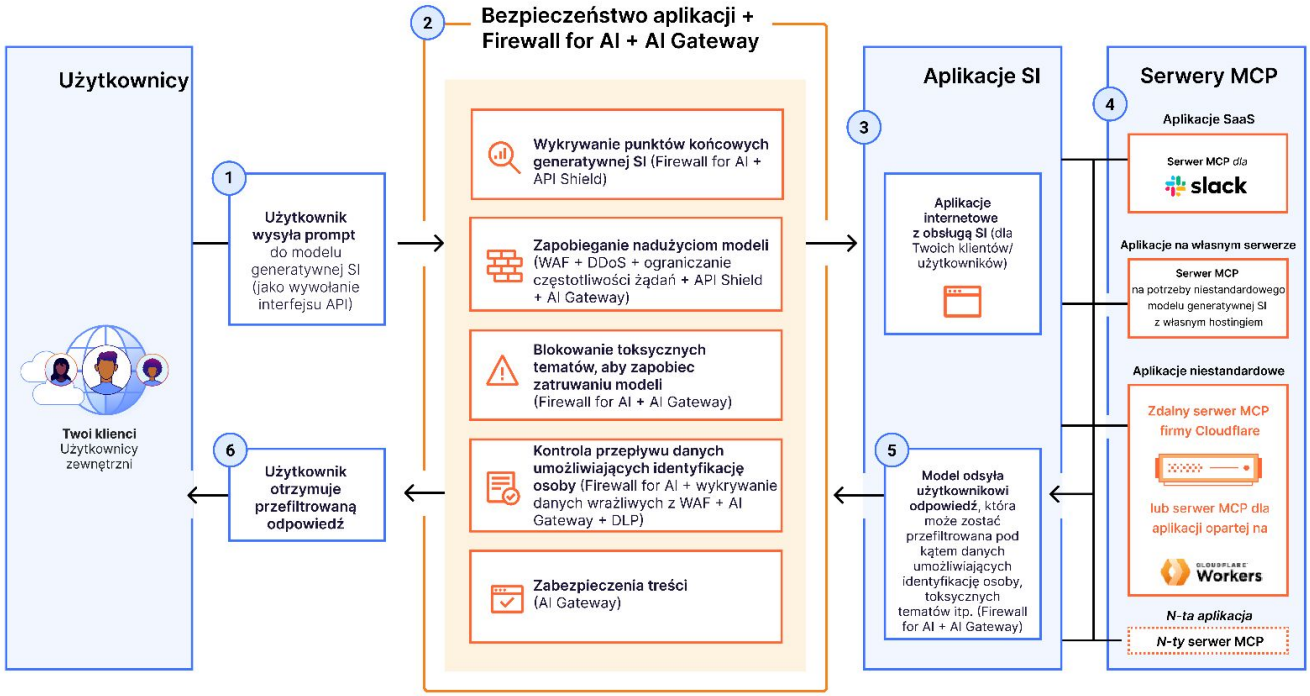
Portale serwerów MCP zabezpieczające komunikację SI z zasobami

- **Widoczność** — agreguj wszystkie dzienniki żądań protokołu MCP (Model Context Protocol) na potrzeby audytu i analizy. Przeglądaj i zatwierdzaj każdy serwer MCP przed dodaniem do portalu.
- **Uwierzytelnianie** — uwierzytelniaj dostęp użytkowników do portalu na podstawie tożsamości. Ogranicz dostęp do serwerów MCP w oparciu o zasadę minimalnych uprawnień.
- **Połączenia** — połącz wszystkie dostępne serwery MCP za pomocą jednego adresu URL, zamiast konfigurować każdy serwer MCP oddzielnie.
- **Ujednolicone zarządzanie** — egzekwuj stosowanie tych samych szczegółowych zasad dostępu dla połączeń SI oraz dla użytkowników końcowych.

Uwaga: portale serwerów MCP obsługują dowolny serwer MCP, w tym (ale nie tylko) zdalne serwery MCP zbudowane lub wdrożone na platformie Cloudflare. Ta funkcja jest dostępna jako kontrola dostępu do sieci w modelu Zero Trust (ZTNA).

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

Chroń aplikacje i obciążenia wykorzystujące SI dzięki niezależnym od modelu, wbudowanym mechanizmom bezpieczeństwa Cloudflare



Chroń publicznie dostępne systemy SI za pomocą zabezpieczeń aplikacji oraz rozwiązania Firewall for AI w następujących celach:

- **Wykrywanie punktów końcowych generatywnej SI** — automatycznie wykrywaj wszystkie modele SI oraz interfejsy API w ramach swoich zasobów sieciowych.
- **Ochrona modeli SI przed nadużyciami** — korzystaj z dedykowanego rozwiązania Firewall for AI, aby blokować ataki typu prompt injection, zatruwanie modeli, nadmierne wykorzystanie oraz inne zagrożenia mogące omijać tradycyjne zabezpieczenia.
- **Kontrola przepływu danych umożliwiających identyfikację osoby** — skanuj prompty użytkowników i odpowiedzi modeli, aby zapobiec ujawnieniu danych wrażliwych i zachować zgodność z przepisami.
- **Zabezpieczenia treści —** blokuj niebezpieczne lub toksyczne prompty z wykorzystaniem zintegrowanych modeli, takich jak Llama Guard. Twórz niestandardowe reguły WAF, aby łatwo blokować lub rejestrować podejrzane interakcje SI.

Chroń tworzoną przez siebie SI za pomocą platformy programistycznej oraz rozwiązania AI Gateway

- **Ujednolicona płaszczyzna zarządzania SI —** zarządzaj wszystkimi aplikacjami SI z jednego pulpitu nawigacyjnego. Przekierowuj żądania, zapisuj odpowiedzi w pamięci podręcznej, kontroluj koszty i monitoruj wydajność.
- **Chroń dane uwierzytelniające na brzegu sieci —** bezpiecznie przechowuj klucze interfejsu API i tajne dane na brzegu sieci, zapobiegając ich ujawnieniu po stronie klienta oraz ułatwiając rotację kluczy między dostawcami.
- **Egzekwuj zabezpieczenia treści** — automatycznie identyfikuj i blokuj lub usuwaj szkodliwe treści oraz dane umożliwiające identyfikację osoby w promptach i odpowiedziach.

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

Cloudflare jest jedynym dostawcą, który zapewnia ochronę zarówno publicznie dostępnych, jak i prywatnych środowisk SI

Wprowadzaj odpowiednie zabezpieczenia, aby z pełnym zaufaniem wdrażać rozwiązania z zakresu SI, dzięki czemu bezpieczeństwo będzie wspierać innowacje, a nie je utrudniać.

- **Ochrona ujednoliconego ekosystemu SI** — złożone stosy zabezpieczeń zwiększają ryzyko. Używaj jednej platformy, aby chronić dane i zapewnić zgodność z przepisami w całym cyklu życia SI.
- **Globalna architektura odporna na przyszłe wyzwania** — już dziś zapobiegaj jutrzejszym problemom dzięki sieci odpornej na zagrożenia kwantowe, skalowalnej dla dowolnych wolumenów ruchu, stale dostosowującej się do nowych zagrożeń oraz możliwej do programowania pod nowe scenariusze zastosowań.
- **Zabezpieczenia oparte na SI** — nasze mechanizmy obronne oparte na SI analizują prompty i odpowiedzi w celu wykrywania zagrożeń w czasie rzeczywistym.
- **Potwierdzone przywództwo w dziedzinie SI** — wprowadzaj innowacje z pełnym zaufaniem na platformie, której ufa 80% spośród 50 czołowych firm z sektora generatywnej SI.
- **Wdrożenie niezależne od modelu** — środki kontroli bezpieczeństwa działają dla wszystkich modeli SI w Twoim środowisku, zapewniając ujednolicone podejście do zarządzania wdrożeniami SI.

Co mówią klienci

indeed

Największa na świecie witryna z ofertami pracy
Zapoznaj się ze studium przypadku

Wykrywaj i kontroluj szarą strefę SI

Równolegle z projektem zastąpienia VPN

APPLIED

Technologie ubezpieczeniowe
Zapoznaj się ze studium przypadku

Izoluj publiczne narzędzia oparte na generatywnej SI, takie jak ChatGPT,

aby blokować kopiowanie i wklejanie danych wrażliwych

Firma oferująca rozwiązania SaaS obsługujące SI

Ochrona danych umożliwiających identyfikację osoby

poprzez uniemożliwienie klientom przesyłania informacji wrażliwych do publicznie dostępnych punktów końcowych generatywnej SI

Cyndx

Fintech oparty na SI

95-procentowa obniżka kosztów wnioskowania

dzięki wykorzystaniu rozwiązań Cloudflare do buforowania i uruchamiania odpowiedzi od dostawców modeli SI

Omów potrzeby Twojej organizacji w zakresie bezpieczeństwa SI?

Porozmawiaj z ekspertem

1. Badanie Manage Engine z 2025 roku: źródło
2. Raport IBM Cost of a Data Breach 2025: źródło

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