

Zapewnij bezpieczeństwo korzystania przez pracowników z generatywnej i agentowej SI

Udostępnij swoim zespołom możliwość bezpiecznego korzystania z dowolnych narzędzi SI dzięki zabezpieczeniom dostępnym na platformie SASE firmy Cloudflare.

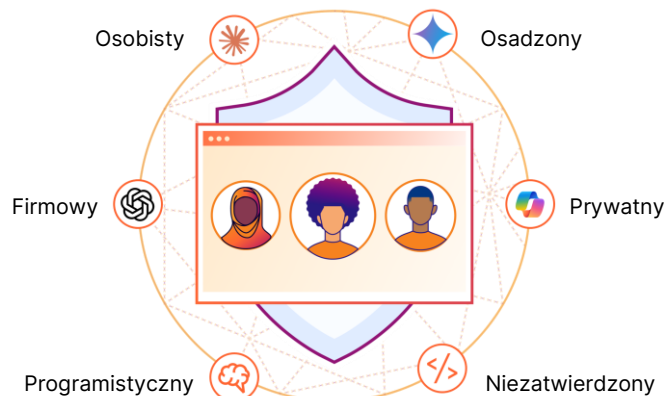
Odzyskaj kontrolę i zwiększ produktywność

Pośpiech we wdrażaniu sztucznej inteligencji podwyższa ryzyko wystąpienia wycieków danych, naruszeń zgodności z przepisami i innych zagrożeń, a także powiększa powierzchnię narażenia na atak. Z kolei zablokowanie inicjatyw związanych z SI powoduje utratę przewagi nad konkurencją, a eksperymentowanie z rozwiązaniami punktowymi jedynie zwiększa złożoność.

Cloudflare zabezpiecza korzystanie ze sztucznej inteligencji przez Twoją organizację, zwiększając widoczność, minimalizując ryzyko i zapewniając całościową ochronę danych w różnych środowiskach:

- **Odkryj szarą strefę SI** i zarządzaj zasadami dla wszystkich zatwierdzonych i niezatwierdzonych narzędzi SI.
- **Wzmocnij zarządzanie SI** za pomocą kontroli dostępu opartej na tożsamości i zarządzania stanem.
- **Zapobiegaj utracie danych**, blokując poufne informacje w promptach użytkowników, wymuszając zabezpieczenia tematyczne i skanując narzędzia SI pod kątem błędnych konfiguracji.

Rozszerz zakres objęty rozwiązaniami Cloudflare, aby bezpiecznie wdrażać środowisko SI, niezależnie od tego, czy Twoja strategia w zakresie sztucznej inteligencji zakłada ograniczenie zastosowań do konkretnych aplikacji, czy też eksperymentowanie z szerszym spektrum różnorodnych narzędzi.



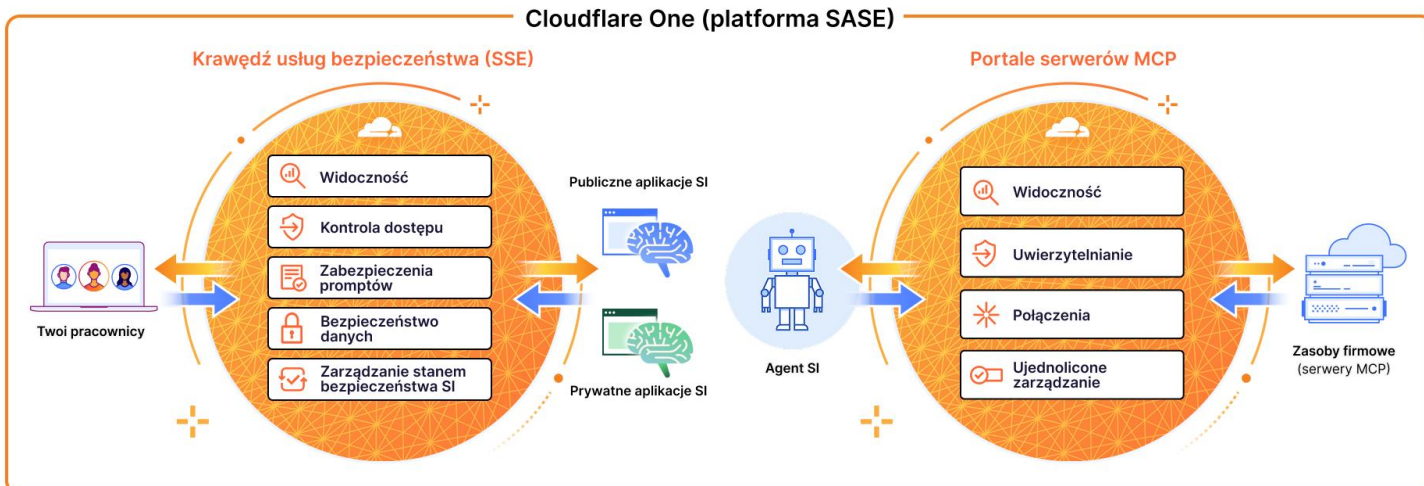
Dlaczego warto użyć platformy SASE do zapewnienia pracownikom bezpieczeństwa podczas korzystania z SI?

Platforma krawędzi usługi bezpiecznego dostępu (Secure Access Service Edge, SASE) firmy Cloudflare umiejscawia się pomiędzy Twoimi pracownikami a narzędziami SI. Dzięki temu stanowi ona dla wielu osób idealny punkt wyjścia do rozpoczęcia bezpiecznego korzystania ze sztucznej inteligencji.

Niezależnie od tego, czy chodzi o pracowników rozmawiających z ChatGPT, czy też o agentów SI zbierających informacje z zasobów korporacyjnych, platforma SASE firmy Cloudflare zapewnia spójne mechanizmy kontroli bezpieczeństwa.

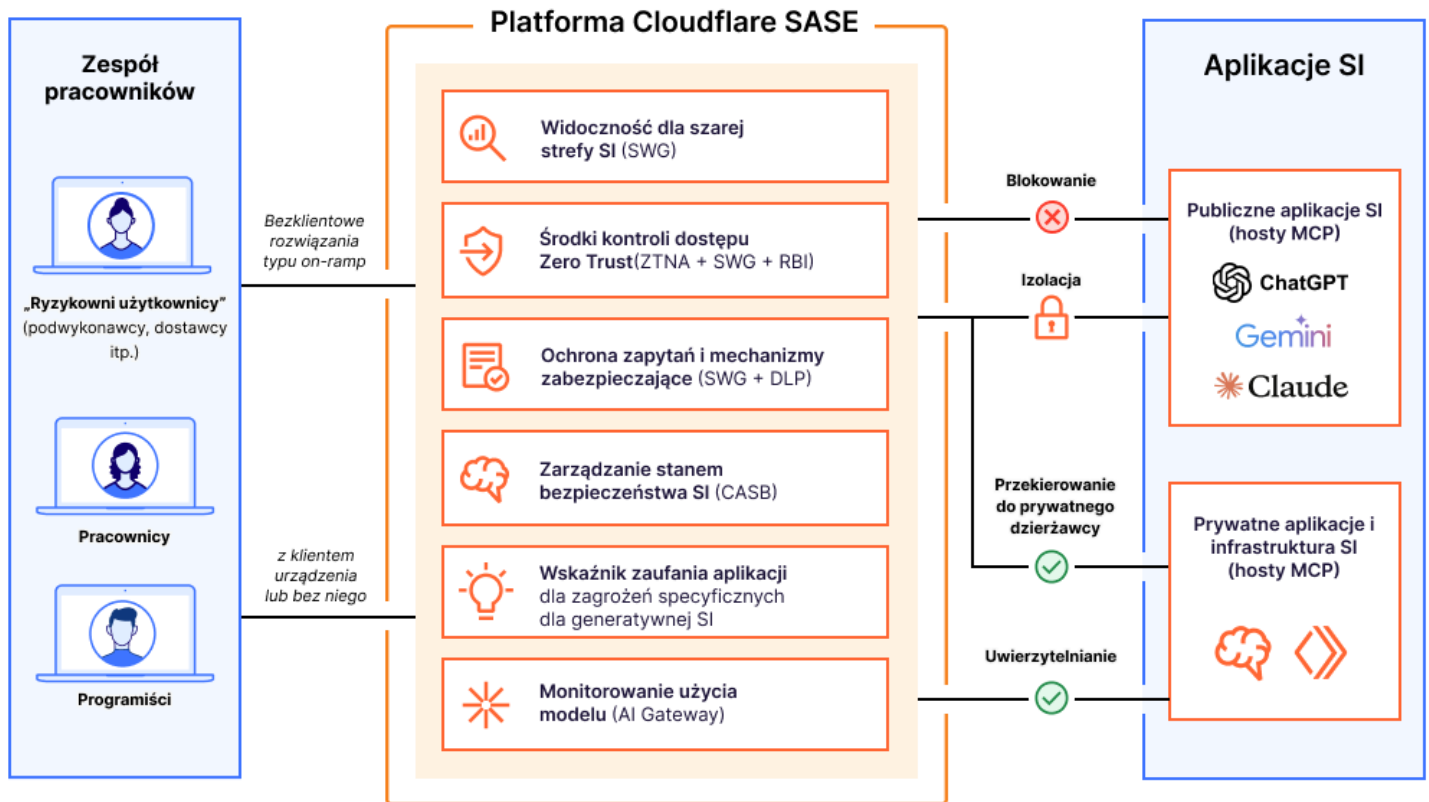
Zabezpiecz komunikację generatywnej i agentowej SI

Platforma SASE firmy Cloudflare oferuje ujednolicony panel kontrolny i płaszczyznę sterowania do zarządzania interakcjami człowiek-SI oraz maszyna-maszyna w całej organizacji.



W przeciwieństwie do innych dostawców SASE firma Cloudflare pomaga również łączyć i chronić publicznie dostępne aplikacje i zasoby wykorzystujące sztuczną inteligencję (takie jak chatbot SI na Twojej stronie internetowej lub mechanizmy rekomendacji).

Chroń komunikację użytkowników z aplikacjami generatywnej SI dzięki kontroli wykorzystania SI na platformie SASE firmy Cloudflare



- **Widoczność:** odkrywaj 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:** zatrzymaj ujawnianie poufnych danych dzięki wspomaganej przez SI [ochronie przed wyciekiem danych \(DLP\)](#) obejmującej zakres dane umożliwiające identyfikację osoby, kod źródłowy i inne.
- **Zarządzanie stanem bezpieczeństwa SI:** wykonaj integrację z narzędziami generatywnej SI za pośrednictwem interfejsu API (dostępne teraz dla [ChatGPT](#), [Claude](#), [Google Gemini](#)) w celu skanowania pod kątem błędnych konfiguracji za pomocą naszego [brokera zabezpieczeń dostępu do chmury \(CASB\)](#).

Wyniki dotyczące klientów



Największa na świecie witryna z ofertami pracy

Wykrywaj i kontroluj szarą strefę SI
równoległe z realizacją projektu zastąpienia sieci VPN

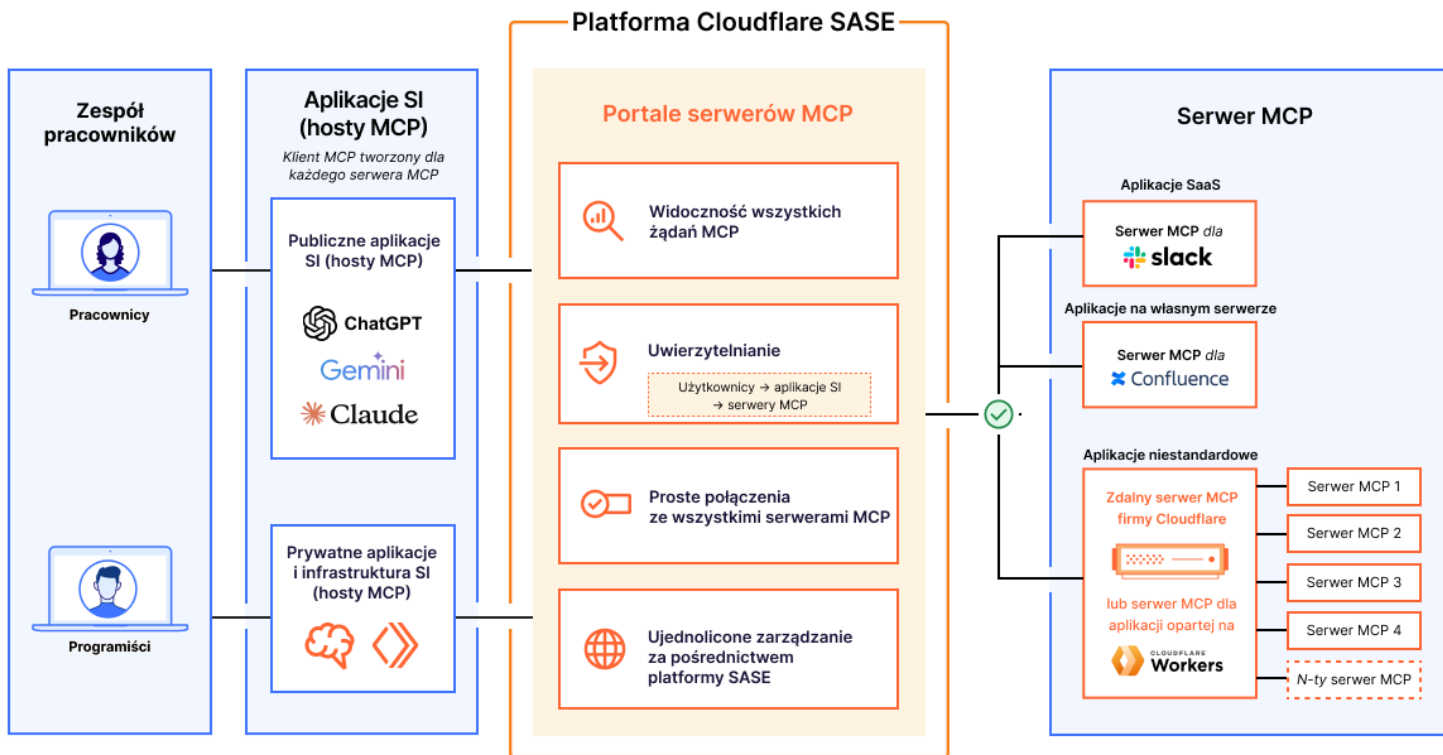


Technologie ubezpieczeniowe

Odizoluj publiczne narzędzia generatywnej SI, takie jak ChatGPT,

aby uniemożliwić kopiowanie i wklejanie poufnych danych

Zabezpiecz komunikację agentowej SI (między SI a zasobami) z portalami serwerów MCP na platformie SASE firmy Cloudflare



- **Widoczność:** agreguj wszystkie dzienniki żądań protokołu (MCP) dla celów 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 na podstawie zasady 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 i dla użytkowników końcowych.

- **Dostosuj narzędzia dla każdego portalu:** wybierz konkretne narzędzia i szablony promptów udostępniane poszczególnym użytkownikom.

Uwaga: portale serwerów MCP firmy Cloudflare 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).

Więcej informacji o naszej wizji znajdziesz w [tym blogu](#).

Chcesz dowiedzieć się, jak Cloudflare może Cię zabezpieczyć podczas korzystania z SI?

Umów się na warsztaty