

Przyspiesz wdrażanie SI dzięki podejściu „security by design”

Sztuczna inteligencja jest już rzeczywistością, a tradycyjne środki cyberbezpieczeństwa po prostu nie nadążają

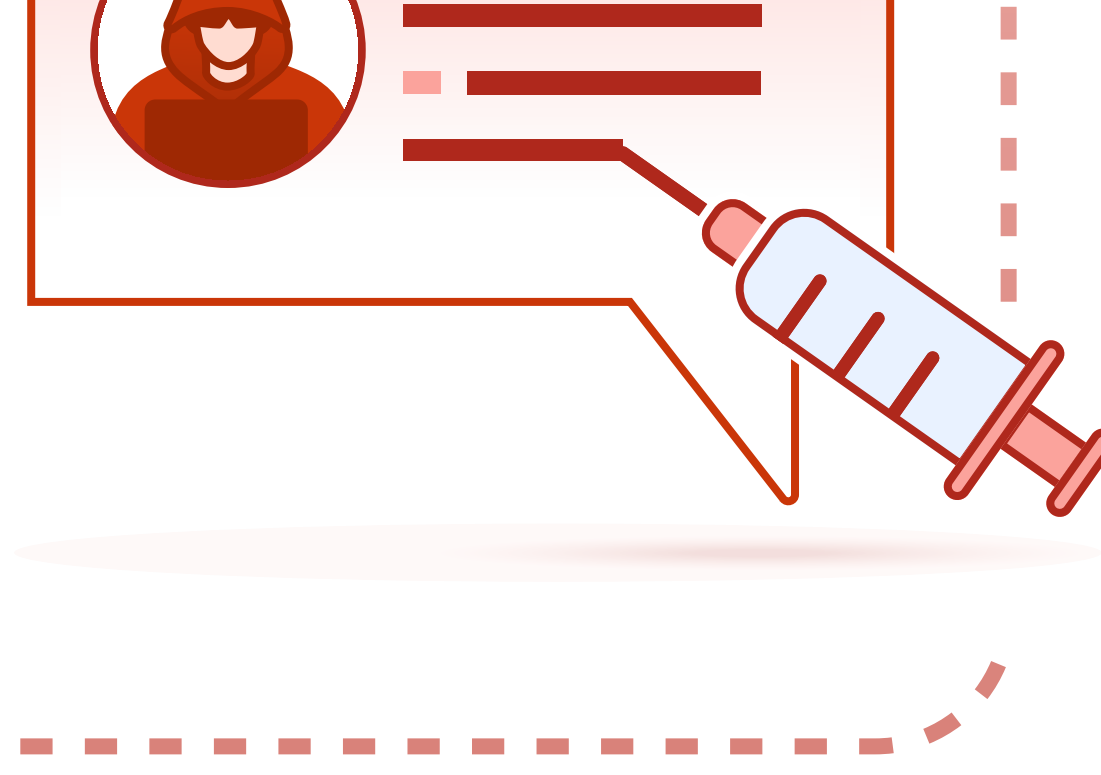


98%

organizacji korzysta z niezatwierdzonych aplikacji, w tym z tzw. szarej strefy SI. Takie obszary nieobjęte kontrolą niosą ryzyko ujawnienia danych oraz naruszenia przepisów dotyczących zgodności¹

50%

skuteczność ataków typu „prompt injection” — zagrożenia uznawanego za najpoważniejsze w zestawieniu OWASP Top 10 dla aplikacji opartych na dużych modelach językowych (LLM)²



97%

organizacji, które doświadczyły incydentów bezpieczeństwa związanych z SI, nie posiadało odpowiednich środków kontroli dostępu do systemów SI³



93%

pracowników przyznaje, że wprowadzało informacje do narzędzi SI bez uzyskania odpowiedniej zgody⁴



Zabezpiecz cały cykl życia SI dzięki Cloudflare

w ramach generatywnej i agentowej SI

Bezpieczeństwo interakcji człowiek–SI



Bezpieczeństwo agentowej SI



Rozszerz widoczność

w aplikacjach SI, punktach końcowych interfejsu API oraz połączeniach agentów SI z serwerami MCP

Zarządzaj ryzykiem

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

Chroń dane

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



Bezpieczeństwo jest wbudowane

już na etapie tworzenia rozwiązań SI w środowisku Cloudflare

Zapewnij bezpieczne korzystanie z generatywnej SI przez pracowników

- Wykrywaj szarą strefę SI
- Oceniaj zagrożenia związane z aplikacjami SI
- Zarządzaj stanem bezpieczeństwa aplikacji SI
- Ograniczaj wprowadzania danych wrażliwych
- Egzekwuj zabezpieczenia w promptach i odpowiedziach

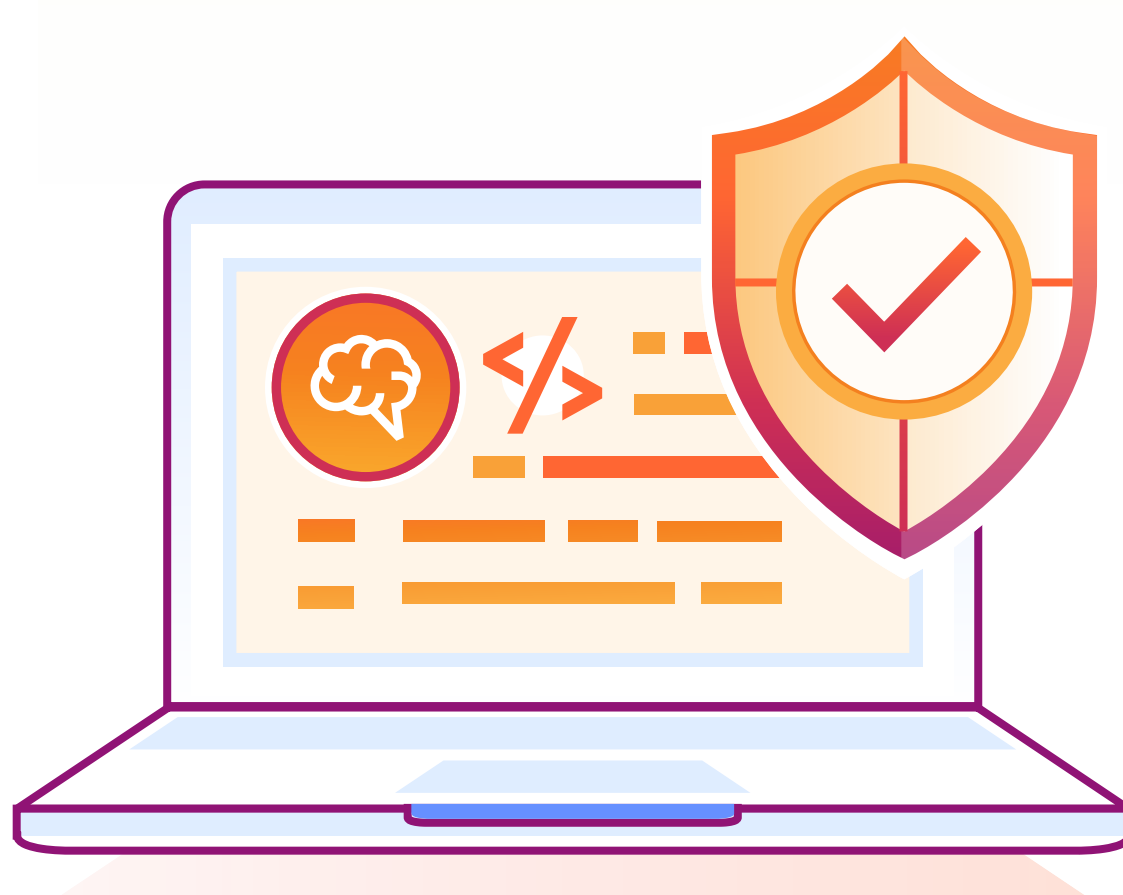
Chroń aplikacje i obciążenia obsługujące SI

- Wykrywaj punktów końcowych szarej strefy SI
- Chroń modele SI i dane treningowe przed nadużyciami
- Zapobiegaj ujawnianiu danych umożliwiających identyfikację osoby w promptach i odpowiedziach
- Egzekwuj moderację treści



Zabezpieczaj wszystko, co tworzysz

- Buduj serwery MCP z wbudowanymi funkcjami uwierzytelniania/autoryzacji
- Rejestruj i ograniczaj żądania/odpowiedzi modelu SI, wykorzystanie tokenów i kosztów
- Zapobiegaj przerwom w działaniu usług dzięki mechanizmom modeli rezerwowych i ograniczaniu częstotliwości żądań



Czym wyróżnia się Cloudflare?

Kompleksowa ochrona w całym cyklu życia SI

Jedna platforma do zabezpieczania komunikacji człowiek–SI oraz SI–zasoby, od etapu tworzenia po wdrożenie.

Wbudowane zabezpieczenia SI w czasie rzeczywistym

Zabezpiecz prompty i odpowiedzi SI w czasie rzeczywistym dzięki środkom kontroli obejmującym publiczne i prywatne środowiska SI.

Globalna architektura SI odporna na przyszłe wyzwania

Korzystaj z naszej globalnej sieci do spójnego egzekwowania zasad na brzegu sieci, ze skalowalnością i wydajnością wymaganą przez sztuczną inteligencję.

Wdrożenie niezależne od modelu

Środki kontroli bezpieczeństwa działają dla wszystkich modeli SI w Twoim środowisku, zapewniając ujednolicone podejście do zarządzania wdrożeniami SI.

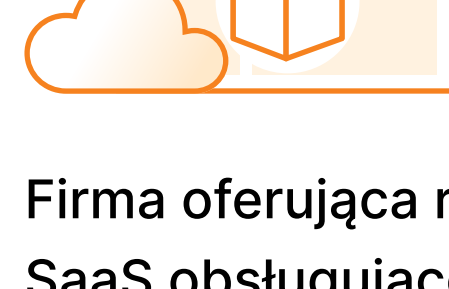
Studia przypadku dotyczące klientów



Największa na świecie witryna z ofertami pracy

Wykrywa i kontroluje szarą strefę SI

równolegle z projektem modernizacji dostępu zdalnego



Firma oferująca rozwiązania SaaS obsługujące SI

Ochrona danych umożliwiających identyfikację osoby

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



Firma fintechowa oparta na SI

Koszty wnioskowania niższe o 95%

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

Dowiedz się, jak Cloudflare może zabezpieczyć proces wdrażania SI

Zapoznaj się z przypadkami użycia

1. Varonis, 2025 State of Data Security
2. Liu, S., Wang, Z., Chen, Y., Deng, G., Liu, Y., & Liu, Y. (2024). Automatic and Universal Prompt Injection Attacks against Large Language Models.
3. IBM, 2025 Cost of a Data Breach
4. ManageEngine, The Shadow AI Surge in Enterprises

© 2025 Cloudflare, Inc. Wszelkie prawa zastrzeżone. CLOUDFLARE® i logo Cloudflare są znakami towarowymi firmy Cloudflare. Wszelkie nazwy innych firm, nazwy produktów i logo mogą być znakami towarowymi odpowiednich firm, z którymi są one powiązane.

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

REV/BDES-8274.2025OCT13