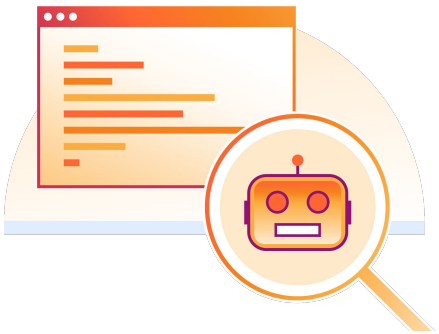
CLOUDFLARE

KRÓTKI OPIS PRODUKTU

Cloudflare Bot Management

Zablokuj złośliwe boty i zarządzaj botami SI bez konieczności stosowania CAPTCHA.



Złośliwe boty ukrywają się w Twoim ruchu, negatywnie wpływając na przychody i doświadczenia użytkowników.

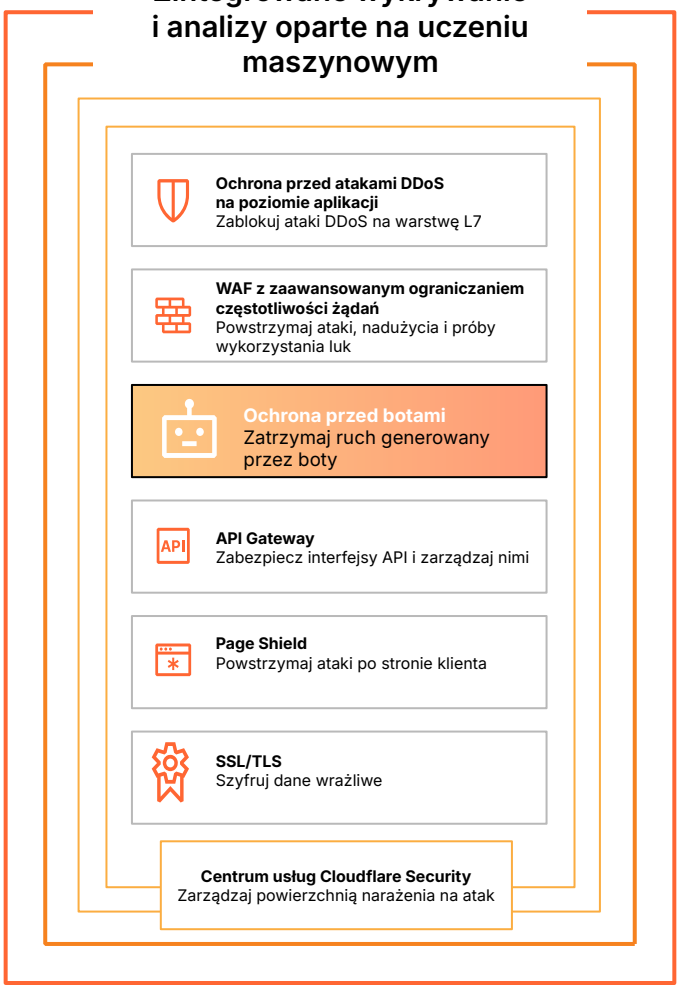
30% ruchu aplikacji w Internecie to ruch zautomatyzowany[1]. Tradycyjne zabezpieczenia, takie jak heurystyki oparte na lokalizacji geograficznej i adresach IP, a także testy CAPTCHA, są łatwo omijane przez nowoczesne boty. To bardzo frustruje prawdziwych użytkowników.

Dzięki wglądowi w **ok. 20%** zasobów sieciowych nikt nie identyfikuje tak wielu robotów indeksujących SI i botów wyszukiwarek, jak Cloudflare[2].

Rozwiązanie **Cloudflare Bot Management** pomaga organizacjom zarządzać botami i robotami indeksującymi SI oraz ruchem generowanym przez boty do aplikacji internetowych i mobilnych bez użycia CAPTCHA. Zezwalaj zweryfikowanym botom i zgodnym robotom indeksującym SI na dostęp do aplikacji, jednocześnie blokując i zatrzymując elementy niezgodne i złośliwe. To kluczowa funkcja w naszym portfolio zabezpieczeń aplikacji.

Korzyści oferowane przez produkt

- Ochrona przed oszustwami, stratami finansowymi i utratą reputacji marki
- Lepsze doświadczenia w zakresie aplikacji internetowych i mobilnych
- Niezależność od niechcianych robotów indeksujących SI i botów wyszukiwania



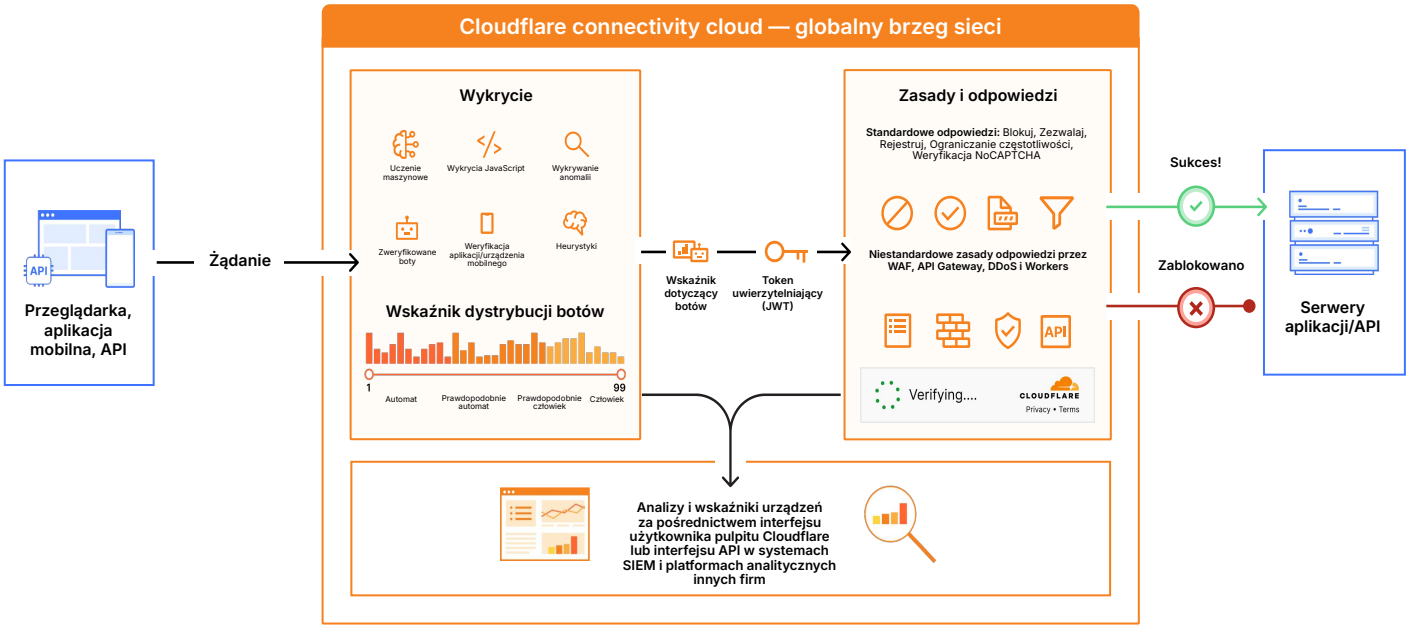
Rysunek 1: rozwiązanie Cloudflare Bot Management zintegrowane z naszym portfolio zabezpieczeń aplikacji

Źródła

1. Dane Cloudflare Radar, 2024 r.
2. W3techs, statystyki użytkowania i udziały w rynku usług odwrotnego serwera proxy, 2025 r.

Jak działa Cloudflare Bot Management?

Cloudflare łączy wielowarstwowe wykrywanie, wykorzystujące globalne i specyficzne dla aplikacji uczenie maszynowe, JavaScript po stronie klienta, urządzenia mobilne oraz heurystyki w celu utworzenia pojedynczego wskaźnika dotyczącego botów przypisywanego do każdego żądania HTTP. Wskaźnik dotyczący botów określa prawdopodobieństwo, że dane żądanie pochodzi od bota. Jest on używany na potrzeby odpowiedzi standardowych, takich jak blokowanie lub zezwalanie, a także w zasadach odpowiedzi niestandardowych za pośrednictwem innych produktów Cloudflare. Analityka botów, w tym wskaźniki dotyczące botów, metadane żądań HTTP i inne dane, są dostępne w interfejsie użytkownika pulpitu Cloudflare lub za pośrednictwem interfejsu API Cloudflare w narzędziach innych firm.



Rysunek 2: przykładowa ścieżka żądania w ramach Cloudflare Bot Management

Kluczowe możliwości rozwiązania Cloudflare Bot Management

Przejęcia kont i nadużycia

Chroń się przed atakami typu zero-day dzięki modelom opartym na uczeniu maszynowym (ML), które wykrywają luki w zabezpieczeniach szybciej niż zostaną one publicznie ujawnione. Zabezpiecz systemy przed rekordowymi atakami DDoS, chroń wrażliwe dane, ograniczaj ryzyko po stronie klienta i monitoruj łańcuch dostaw oprogramowania Twojej aplikacji internetowej.

Ochrona przed botami i oszustwami

Chroń użytkowników przed przejęciami kont i blokuj złośliwe boty, które negatywnie wpływają na komfort użytkowania. Powstrzymaj złośliwe sieci botów, ataki typu „credential stuffing" i „card stuffing", pozyskiwanie danych oraz ataki typu „inventory hoarding", łącząc modele uczenia maszynowego z danymi o klientach i sieci oraz analizą zagrożeń.

Zarządzanie robotami indeksującymi i botami SI

Zyskaj większą kontrolę nad treścią i kosztami, blokując roboty indeksujące SI, pobierając od nich opłaty lub umieszczając je w nieskończonych pętlach. Zyskaj wgląd we wzorce zapytań i zgodność z zasadami w pliku robots.txt. Ta funkcja jest dostępna dla wszystkich klientów Cloudflare.

Kluczowe możliwości	
Mechanizmy wykrywania	
Uczenie maszynowe	Nasz globalny model uczenia maszynowego jest trenowany na całym globalnym ruchu sieciowym Cloudflare, który obsługuje miliardy żądań dziennie, aby identyfikować ruch zautomatyzowany i generowany przez ludzi. Jest to uwzględnione w naszym ogólnym wskaźniku dotyczącym botów. Klienci są automatycznie aktualizowani do najnowszego modelu.
Wykrywanie anomalii	Nasze modele anomalii behawioralnych, oparte na uczeniu nienadzorowanym, ustalają bazowe wzorce ruchu specyficzne dla aplikacji i kalibrują progi reguł w celu identyfikacji nietypowych zachowań botów, w miarę jak wzorce ruchu klientów zmieniają się w czasie. Jest to uwzględnione w naszym ogólnym wskaźniku dotyczącym botów.
Heurystyki	Do ich identyfikacji wykorzystujemy znane wzorce złych zachowań botów pochodzące z wcześniejszego ruchu generowanego przez boty. Regularnie aktualizujemy nasze heurystyki dla wszystkich klientów. Jest to uwzględnione w naszym ogólnym wskaźniku dotyczącym botów.
Zweryfikowane boty i boty SI	Nasz katalog botów identyfikuje znane identyfikatory wykrywania botów, które realizują uzasadnione funkcje i działają w przejrzysty sposób jako zweryfikowane boty, zgodnie z polityką zweryfikowanych botów Cloudflare. Mamy oddzielną kategorię dla rozpoznanych botów SI, które mogą, ale nie muszą respektować plik robots.txt i ukrywać swoje działanie przed Twoimi aplikacjami.
Wykrywanie JavaScript	Moduł wykrywania JavaScript identyfikuje bezobsługowe przeglądarki oraz inne złośliwe odciski cyfrowe poprzez lekkie, niewidoczne wstrzykiwanie kodu JavaScript po stronie klienta dla każdego żądania. Przestrzegamy bardzo rygorystycznych standardów prywatności i nie zbieramy żadnych danych umożliwiających identyfikację osoby podczas tego procesu.
Wskaźnik dotyczący botów	Wskaźnik dotyczący botów pozwala ograniczyć liczbę reguł definiowanych w celu wychwycenia większości botów i uniknąć konieczności tworzenia reguły dla każdego identyfikatora lub typu bota. Wskaźnik ten łączy dane z naszych mechanizmów wykrywania, generując wynik od 1 do 99, który wskazuje prawdopodobieństwo, że dane żądanie pochodzi od bota. Wartość 1 oznacza żądania zdecydowanie automatyczne, a 99 — zdecydowanie ludzkie.
Weryfikacja urządzenia za pomocą pakietów SDK urządzeń mobilnych	Te zestawy SDK, dostępne dla wszystkich głównych platform aplikacji mobilnych, w tym Android, iOS, React Native, Unity i innych, weryfikują integralność aplikacji, wykrywają niebezpieczne środowiska i uwierzytelniają ruch API (za pomocą samodzielnie dostarczonych lub zatwierdzonych przez Cloudflare tokenów kryptograficznych).
Zasady i odpowiedzi	
Odpowiedzi standardowe	Skonfiguruj blokowanie, zezwalanie, rejestrowanie, ograniczanie częstotliwości lub różne łatwe w użyciu weryfikacje jako odpowiedzi na ruch generowany przez boty zidentyfikowany przez nasze mechanizmy wykrywania.
Zasady odpowiedzi niestandardowych	Włącz sygnały Cloudflare Bot Management do zasad w innych produktach Cloudflare, takich jak Cloudflare WAF i DDoS, oraz twórz niestandardowe akcje za pomocą Workers.
Analiza danych	
Pulpit nawigacyjny Cloudflare	Przeglądaj aktywność botów do 30 dni wstecz i filtruj według wartości wskaźnika dotyczącego botów oraz innych filtrów botów, ruchu generowanego przez boty i zapytań. Pętla opinii bota pozwala klientom zgłaszać Cloudflare wszelkie wyniki fałszywie dodatnie lub fałszywie ujemne w celu dalszego zbadania.
Narzędzia innych firm (SIEM, jeziora danych, narzędzia analityczne itp.)	Analizuj sygnały Cloudflare Bot Management we wszystkich aplikacjach na jednym pulpicie, korzystając z usług Cloudflare Security Analytics. Przeglądaj dodatkowe dane dziennika w Log Explorer i łącz dane innych firm z danymi Cloudflare w systemie SIEM lub na platformie analitycznej innej firmy za pomocą funkcji Log Push.

Chcesz zobaczyć więcej? Zarejestruj się na naszą serię demonstracyjną dotyczącą bezpieczeństwa aplikacji.