

API Shield firmy Cloudflare

Zarządzaj i zabezpieczaj interfejsy API, które stymulują działalność biznesową

Wyzwania związane z nowoczesnymi interfejsami API

Na celowniku atakujących

Interfejsy API mają bardzo istotne znaczenie. Aż 58% dynamicznego ruchu HTTP w sieci Cloudflare jest powiązane z interfejsami API.

Interfejsy API oferują ekscytujące możliwości biznesowe, umożliwiając szybsze dostarczanie produktów i poprawę doświadczeń klientów. Obecnie liderzy ds. bezpieczeństwa i IT muszą równoważyć ochronę swoich interfejsów API oraz aplikacji internetowych, nie spowalniając przy tym tempa innowacji.

Zespoły ds. bezpieczeństwa i IT muszą zabezpieczyć dane wrażliwe klientów, umożliwiając jednocześnie prowadzenie działalności operacyjnej w ramach zasobów aplikacji internetowych i interfejsów API.

W końcu chodzi o zaufanie klientów.



API Shield firmy Cloudflare

Klienci mogą wykrywać, zabezpieczać i upraszczać zabezpieczenia swoich publicznych interfejsów API oraz zarządzanie nimi, konsolidując ochronę aplikacji internetowych i interfejsów API na brzegu sieci Cloudflare.

API Shield wchodzi w skład portfolio narzędzi bezpieczeństwa aplikacji firmy Cloudflare, które dodatkowo powstrzymują boty, udaremniają ataki DDoS oraz blokują ataki na aplikacje, jak również monitorują pod kątem ataków na łańcuch dostaw.



Zagrożenia związane z ukrytymi interfejsami API

Zespoły programistyczne często publikują nowe interfejsy API bez informowania o tym działu IT, przez co interfejsy te działają w cieniu — bez zarządzania i zabezpieczeń.



Obawy dotyczące uwierzytelniania, utraty danych i nadużyć

Po wykryciu interfejsów API należy je zabezpieczyć przed atakami i nadużyciami poprzez wdrożenie mechanizmów uwierzytelniania, walidacji schematów, ochrony przed nadużyciami API oraz wykrywania eksfiltracji danych.



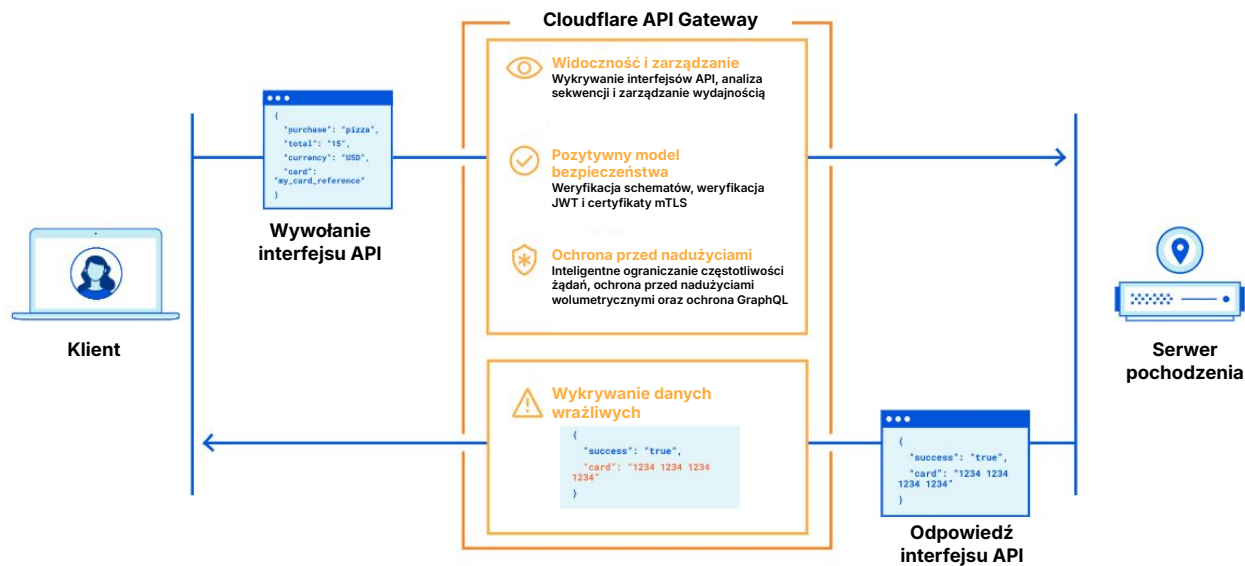
Monitorowanie wydajności interfejsów API

Ponieważ interfejsy API stymulują działalność biznesową, po ich zmonitorowaniu i zabezpieczeniu firmy muszą skontrolować ich wydajność — śledzić liczbę żądań na każdy punkt końcowy, wskaźniki błędów i opóźnienie.

API Shield firmy Cloudflare

Zarządzaj i zabezpieczaj interfejsy API, które stymulują działalność biznesową

Kluczowe możliwości	
Wykrywanie interfejsów API i zarządzanie nimi	
Wykrywanie i uczenie schematów	Wykrywaj aktywnie używane punkty końcowe interfejsu API oraz powiązane z nimi schematy za pomocą modeli opartych na uczeniu maszynowym i heurystykach.
Analiza sekwencji i wydajności	Odkryj najważniejsze sekwencje zachowań w wywołaniach interfejsu API oraz przeanalizuj wydajność punktów końcowych interfejsu API (np. żądania, opóźnienie, wskaźnik błędów, rozmiar odpowiedzi itp.).
Portal dla programistów i zarządzanie	Zarządzaj interaktywną dokumentacją API i hostuj ją w swojej domenie dzięki Cloudflare Pages.
Poziom bezpieczeństwa interfejsów API	
Wykrywanie ataków BOLA	
Stan uwierzytelniania	Korzystaj ze skanów pod kątem zagrożeń identyfikujących błędne konfiguracje uwierzytelniania w interfejsach API, takie jak brak uwierzytelniania czy uwierzytelnianie mieszane (gdy tylko niektóre wywołania interfejsu API do punktu końcowego wymagają uprawnień dostępu), a także ostrzegają o nich.
Wykrywanie danych poufnych	Wykrywaj dane wrażliwe w odpowiedziach API opuszczających źródło i wysyłaj alerty dla każdego punktu końcowego.
Ochrona środowiska wykonawczego API	
Weryfikacja uwierzytelniania	Uwierzytelniaj i weryfikuj ruch API za pomocą certyfikatów mTLS, tokenów internetowych JSON (JWT), kluczy interfejsu API i tokenów OAuth 2.0, aby blokować żądania od nieautoryzowanych klientów.
Weryfikacja schematów	Używaj schematów API do akceptacji prawidłowych wywołań interfejsu API oraz do blokowania niewłaściwie sformułowanych żądań i anomalii HTTP. Stanowi to uzupełnienie negatywnego modelu bezpieczeństwa Cloudflare WAF w celu zapewnienia kompleksowej ochrony.
Ochrona przed nadużyciami REST i GraphQL	Zapobiegaj nadużyciom wolumetrycznym i sekwencyjnym dzięki sugestiom ograniczania częstotliwości żądań w oparciu o sesje dla poszczególnych punktów końcowych. Rozszerz ochronę przed atakami DoS na punkty końcowe GraphQL.



Rysunek 1: Architektura Cloudflare API Shield

Cloudflare liderem w obszarze cyberbezpieczeństwa

Portfolio narzędzi bezpieczeństwa aplikacji firmy Cloudflare było wielokrotnie nagradzane za swoją skuteczność i szeroki zakres ochrony. Cloudflare została uznana za lidera w najnowszym raporcie „Forrester Wave: Web Application Firewalls”. Firma Gartner przyznała Cloudflare tytuł „Customers’ Choice Leader” w kategorii rozwiązań zapewniających ochronę przed atakami DDoS w raporcie Gartner® Peer Insights™ „Voice of the Customer: DDoS Mitigation Solutions” z 2023 roku. Firma Forrester przyznała Cloudflare tytuł „Strong Performer” w raporcie „The Forrester Wave™: Bot Management Software” za 3. kwartał 2024 r. Firma IDC uznała Cloudflare za jednego z głównych graczy w raporcie „2024 IDC MarketScape for Web Application and API Protection (WAAP) Enterprise Platforms”.